〔美〕I. 格罗斯曼
W. 迈格努斯 著

群和它的图象表示



科 学 普 及 出 版 社

群和它的图象表示

〔美〕I. 格拉斯曼　W. 迈格努斯　著
胡复　唐松　译

科学普及出版社

内 容 提 要

群论是现代数学的一个重要分支，它是研究代数方程、几何变换以及拓扑学和数论问题的强有力工具；在物理学、化学、结晶学、图案设计等其他领域中都有应用。但由于群论概念的高度抽象性以及它在其他研究领域的深刻应用，难以向群众作通俗介绍；本书由于引进了群的几何形象——群的图象，因而把抽象群具体化、形象化了，较为通俗，已被译成多种文字。

本书涉及群的几种定义法、子群、正规子群、四元数群、置换群、对称群、交代群、道路群等，可供高中及大学学生及有关研究人员参考。

GROUPS AND THEIR GRAPHS

by

I. GROSSMAN W. MAGNUS

* * *

群和它的图象表示

〔美〕I. 格拉斯曼 W. 迈格努斯 著

胡 复 唐 松 译

封面设计：窦桂芳

*

科学普及出版社出版（北京白石桥紫竹院公园内）

新华书店北京发行所发行 各地新华书店经售

中国科学院印刷厂印刷

*

开本：787×1092 毫米 1/32 印张：6 3/4 字数：154 千字

1981 年 2 月第 1 版 1981 年 2 月第 1 次印刷

印数：1—10,500 册 定价：0.58 元

统一书号：13051·1162 本社书号：0192

序　　言

中小学学生常有这种观念，认为数学仅仅涉及数和测量．然而，数学不只是应用于象记账和换钱等活动的定量科学；它和逻辑及结构也有深刻的关系．

群论是数学中重要的非定量的分支之一．在数学发展过程中，群的概念虽然产生较晚，但已经获得许多成果．比如说，它已是研究代数方程和几何变换以及拓扑学和数论问题的强有力的工具．

群论有两个显著的特点，一个是它的概念的高度抽象性，另一个是它在其他研究领域中有着深刻的应用．由于只有在数学上相当成熟才能掌握这类抽象概念，只有在理论经过长时期的广泛发展之后才能看到这种实际应用，并且只有通晓其他领域的学生才能掌握这种应用，因此，群论的学习通常都要推迟到学生的数学教育的后期．

对于仅仅学过初等数学的学生，是否也可以学习一点群论的知识呢？也是可以的．本书的目的就在于对这类读者作一介绍．为了克服抽象化所带来的困难，我们引进了群的几何形象——群的图象．这样可以把抽象群具体化，变成对应于群的结构的可见模型．但是，这只不过是为了使读者便于理解我们讲述的定理和概念，而不是打算把它当成进一步阅读和学习的读者提供一个掌握有关数学概念的代用品．

我们承认，我们不能总是用"实际"应用来启发读者．归根到底，我们需要介绍的是数学内容本身．当然，学习的动力还是来自读者，这也是他们自已应该做的贡献．

目　录

第一章 群的引言

群论在十八世纪末始具雏型．十九世纪初，它仍发展缓慢，没受到什么重视，其后，在1830年前后的几年里，通过伽罗华（Galois）和阿贝尔（Abel）关于代数方程的可解性的工作，群论向前大大跃进了，并对整个数学的发展作出了重大贡献．

从那时起，群论中的许多基本概念被精心提炼出来并且推广到许多数学分支．群论在各种不同的领域（象量子力学、结晶学及纽结理论）中都有了应用．

本书主要讨论群及其图象表示．我们的第一个任务就是要阐明"群"是什么意思．

通往群的概念的基本思想是结构（或范型）．下面读者就会看到，列举的一些例子和解释，定义和定理，都可以看成是一个基本主题的各种变化：群及其图象是如何体现并说明一种数学结构的．

虽然现在我们已经用了"群"这个字，却没有告诉读者它的意思是什么．如果一下子就把完整的形式定义端出来，读者也许从一开始就会感到莫名其妙．因此，我们一步一步慢慢来讲群的概念，先举两个例子．

群A 所有整数的集合 $\{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$，把它们看成彼此能够相加的数．换句话说，群A的元素是整数，而我们感兴趣施行的唯一运算是集合中任意两个元素的加法；例如 $2+5=7$．

群B 所有正有理数的集合，把它们看成彼此能够相乘

的数．在这种情形下，集合的元素就是所有能够表成 $\frac{a}{b}$ 形式的数，这里 a 和 b 是正整数，而我们感兴趣施行的唯一运算是集合中任意两个元素的乘法；例如 $\frac{2}{3}\cdot\frac{5}{8}=\frac{5}{12}$.

现在在读者面前已经展示了群的例子，然而他在理解群是什么的大道上仍然没走多远，因为他可能不会立即认识到这些例子中的哪些特点在群的本质结构中是起主要作用的．在我们描述群A和群B时，有着重点的那些字就是为了强调在所有群中出现的基本结构范型．我们可以突出其中的两个特征：

1. 元素的集合 { 群A：所有整数；群B：所有正有理数 }

2. 集合上的一种二元运算 { 群A：任意两个整数的加法；群B：任意两个正有理数的乘法 }

我们把群A和群B的运算称为二元运算，是因为每次运算只涉及两个元素．

一个集合上的二元运算是一种对应，对于集合中的有次序的每一对元素它指定这个集合中的唯一确定的元素．因此在群A中，加法是在整数集合上的二元运算，这是因为，假如 r 与 s 是我们集合中的任意两个元素，则 $r+s$ 也是集合中的一个元素． 如果我们用符号 t 表示元素 $r+s$，我们可以把这段叙述这么说：如果 r 和 s 是我们集合中任意两个元素，则集合中有且仅有一个元素 t，使得 $r+s=t$． 例如，假使我们选 2 和 5 为我们的集合中的两个元素，那么就有集合中唯一的元素 7，使得 $2+5=7$．

群B的二元运算是乘法；这是由于，假如 r 及 s 是我们的（正有理数）集合的两个元素，则有且仅有一个集合中的元素 t，使得 $r\cdot s=t$．（为了得出元素 t 的唯一性，需把相等的有

理数，例如$\frac{4}{8}$与$\frac{1}{2}$，理解为表示同一个数.）假如我们选取$\frac{2}{3}$及$\frac{5}{8}$为我们集合中的两个元素，则存在集合中唯一的元素$\frac{5}{12}$使得$\frac{2}{3}\cdot\frac{5}{8}=\frac{5}{12}$.

要注意，"二元运算"这个概念本身就包含一个相关的集合.这就是为什么我们用"在一个集合上的二元运算"这个词.一对元素以及通过二元运算所指定的对应元素必须全都是同一集合中的元素. 这样我们就看出，群的两个密切相关的特征是：(1)元素的集合，(2)这个集合上的二元运算. 这样两个特征是互相缠绕在一起不能分开的，虽然，我们可能有时候把注意力从一个特征转到另一个特征上较为方便.

刚才我们所考虑的群的二元运算的例子是通常整数的加法，用符号＋表示，以及正有理数的乘法，用·表示. 后面我们会看到，对于不同的群有许多不同的二元运算，有时把这些运算都用同一个符号表示较为方便. 我们就用符号⊗来表示这种没有特殊指定的二元运算.

这个记号使得我们有可能把群A及群B所显示的结构特征(1)和(2)表述为：一个集合S以及S上的一个二元运算⊗.假如r及s是S中任意两个元素，则S中存在唯一的元素t，使得

$$r\otimes s=t.$$

对于群A，⊗表示"整数的加法"这种特殊运算；对于群B，⊗表示"正有理数的乘法".

为了强调二元运算是一种对应，我们再换一种方式来描述我们所讨论过的群. 在群A的情形，我们可以说，对应于任何一对整数r及s，存在唯一整数t. 我们能够用符号写成

$$(r,s)\to t,$$

其中箭头表示"对应于"。在群B的情形，我们可以说，对应于任何一对正有理数 r 及 s，存在唯一的正有理数 t。

为了对一个集合上的二元运算有更广的观点，我们考虑这样的问题：是否一个集合上的二元运算也可以是一个子集上的二元运算？（如果 U 的每个元素也是 S 的元素，我们把集合 U 称为集合 S 的子集。）例如，假定 S 是所有正有理数的集合，U 是由所有正整数组成的子集。首先让我们决定是否除法是 S 上的二元运算。读者很容易证明除法是正有理数集合 S 上的二元运算。如果 r 及 s 是任意两个正有理数，就存在唯一的正有理数 t，使得

$$r \div s = t.$$

现在让我们来考察一下集合 S 上的二元运算除法是否也是正整数子集 U 上的二元运算。显然，如果在子集 U 中我们选择了二个元素比如说2和3，则就不存在任何正整数 t 使得

$$2 \div 3 = t.$$

于是，除法并不是正整数子集 U 上的二元运算，因为存在正整数对，它不对应于第三个正整数。

与这种情况相反，让我们考虑所有整数的集合 S 及所有偶数的子集 U。我们已经看到加法是所有整数的集合 S 上的二元运算。在加法运算下，偶数子集会出现什么情况？当两个偶数相加时，得数也是偶数。换句话说，加法是偶数子集上的二元运算，就象它是整数集合上的二元运算一样。偶数子集 U 中的任意两个元素相加，其和总是 U 中的元素。我们把这种性质说成：偶数子集 U 在加法二元运算下是封闭的。读者能够验证，奇数子集在这个运算下不是封闭的。

我们可把子集在二元运算下的封闭性更一般地说法叙述为：如果 $\otimes$ 是集合 S 上的二元运算，U 是 S 的子集且具有如下性质：当 u 及 v 属于子集 U 时，$u \otimes v$ 就是 U 的元素，则我

们就说U在运算$\otimes$下是封闭的. "封闭"这词提示我们，当把运算$\otimes$限制在U中的元素对上时，运算结果不会弄到U的外面去；所以我们可以把$\otimes$看成是集合U上的二元运算.

第八章中我们将会看到，在讨论"子群"时，这种子集在二元运算下的封闭性质怎样起着关键的作用.

练习 1

(a) 加法是奇正整数的集合上的二元运算吗？

(b) 乘法是奇正整数的集合上的二元运算吗？

(c) 设集合的元素为 $1, i, -1, -i$ (其中 $i=\sqrt{-1}$). 加法是这个集合上的二元运算吗？

(d) 乘法是否是 (c) 中集合上的二元运算？

到现在为止，我们已经看到一个群是一个集合连同这集合上的一种二元运算. 如果r及s是这集合上的任意两个元素，则存在这个集合的唯一元素t使得

$$r\otimes s=t \text{ 或 } (r, s)\to t.$$

"如果r及s是这集合上任意两个元素"这段话并不排除r及s可能表示相同元素；它也没预先假定r及s的特殊次序. 因此，假如r及s是这集合上任意两个元素，则

$$r\otimes s,\ r\otimes r,\ s\otimes s,\ s\otimes r$$

也是这个集合的元素(它们不一定彼此完全不同).

现在就要问：一个群中，$r\otimes s$及$s\otimes r$能够是集合中的不同的元素吗？在群A及群B中，显然$r\otimes s=s\otimes r$总成立. 例如，在群A中，我们有$3+5=5+3$，在群B中我们有$\frac{2}{3}\cdot\frac{7}{2}=\frac{7}{2}\cdot\frac{2}{3}$. 但是，在正有理数集合中以除法为二元运算时，我们就看到，比如$\frac{2}{3}\div\frac{7}{2}\neq\frac{7}{2}\div\frac{2}{3}$. 一般来说，这个

集合中，$r \otimes s \neq s \otimes r$. 因此，元素的次序很重要；在某些集合中，改变或交换元素的次序可以得出不同的结果，即有可能

$$(a, b) \to c \text{ 及 } (b, a) \to d,$$

其中 a, b, c, d 是一个群的元素且 $c \neq d$.

当 $r \otimes s = s \otimes r$ 时，我们就说元素 r 及 s（关于用⊗表示的特殊运算）可交换；如果 $r \otimes s \neq s \otimes r$，我们就说元素 r 及 s（关于这个特殊运算）不可交换. 从现在起，我们事先并不保证在运算⊗之下，有序对 (r, s) 与有序对 (s, r) 对应到相同的元素. 对于每一个情形，我们都要分别检查其可交换性.

考虑到一般我们有必要区别 $r \otimes s$ 及 $s \otimes r$，我们把一个集合及其相关的二元运算的刻划重述如下：对于集合中每个有序的元素对 r 及 s，存在集合中的唯一元素 t 使得

$$r \otimes s = t \text{ 或 } (r, s) \to t.$$

到现在为止，在所有集合及其相关的二元运算的例子中都把数作为元素，把我们熟知的一种算术运算当作二元运算. 但是，我们就会看到，群的元素也可以不是数，而是其他对象，例如运动，置换，函数，几何变换或者一组符号；在这些情形下，相关的二元运算就不具有算术性质.

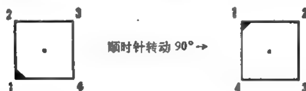


图 1.1

例如，考虑一个正方形可以在平面上围绕通过它的中心的轴自由转动，但是允许的转动只限于使这个正方形和自身重合的转动. 那么，一个允许的转动就是沿顺时针方向转动 90°（见图 1.1）. 让我们用 a 表示这个转动. 另外一些允许

的转动可以是：(1)顺时针转动 180°，我们用 b 表示；(2)顺时针转动 270°，我们用 c 表示.

我们可以把这些转动 a, b, c 看成一个群的元素. 是否我们能够定义一个二元运算使得 $a\otimes b=c$ 有意义呢？一个办法是按下列方式去思考：

顺时针转动 90° 接着 顺时针转动 180°

等价于

顺时针转动 270°，

或者

元素 a 接着元素 b 等于元素 c，

或者

$$a\otimes b=c.$$

把两个元素 a 与 b 同元素 c 联系起来的这个运算可以称为"接着"，也可称为"相继". 对于转动来说，相继这种运算是有意义的. 下面将会看到，对于其他各种可能的群的元素也可以使之有意义.

练习 2 把二元运算理解为"接着"或相继，$b\otimes c$ 表示正方形的转动的集合中的什么转动？$a\otimes c$ 又表示什么转动？

第二章 群 的 公 理

虽然到此为止我们都在讨论集合上的二元运算，但读者不应由此断定，它就是群的唯一特征。事实上，为了使得某个具有二元运算的集合构成一个群，还必须假设：这个二元运算还具有几个涉及这个集合元素的基本性质。刻划这些基本性质的假设，就是所谓的(群的)公理，我们将需要三个这样的公理。我们称它们为：(1) 结合性公理，(2) 单位元素(或恒等元素)公理，(3) 逆元素公理。

可结合性

可结合性是说，若 r, s, t 是集合的任意三个元素，则

$$r\otimes(s\otimes t)=(r\otimes s)\otimes t;$$

也就是说，若 $s\otimes t$ 是集合的元素 x，$r\otimes s$ 是元素 y，则 $r\otimes x=y\otimes t$。

让我们考察前面说过的群 A 和群 B (见第 1 页)。在群 A 中，可结合性就是，对任意三个整数 r, s, t，有

$$r+(s+t)=(r+s)+t.$$

例如，我们有

$$5+(3+8)=5+11=16$$

及

$$(5+3)+8=8+8=16.$$

在群 B 的情况，我们将有

$$r\cdot(s\cdot t)=(r\cdot s)\cdot t.$$

例如，

$$\frac{3}{8}\cdot\left(4\cdot\frac{2}{3}\right)=\frac{3}{8}\cdot\frac{8}{3}=1$$

及

$$\left(\frac{3}{8}\cdot 4\right)\cdot\frac{2}{3}=\frac{3}{2}\cdot\frac{2}{3}=1.$$

我们由初等代数的经验知道，群A和群B的二元运算是可结合的.

现在让我们把除法作为正有理数集合上的二元运算来考虑，看看这时结合性是否也成立. 我们有

$$\frac{3}{2}\div\left(3\div\frac{3}{4}\right)=\frac{3}{2}\div 4=\frac{3}{8},$$

而

$$\left(\frac{3}{2}\div 3\right)\div\frac{3}{4}=\frac{1}{2}\div\frac{3}{4}=\frac{2}{3},$$

所以

$$r\div(s\div t)\neq(r\div s)\div t.$$

这就是说，除法不是正有理数集合上的可结合的二元运算.

那么，不加括号的表达式 $r\otimes s\otimes t$ 的含义是什么？如果 $\otimes$ 表示一个集合上的二元运算，当包含这个集合的三个元素时我们又如何应用它？ 我们能给表达式 $r\otimes s\otimes t$ 一个确定的意义，就是或者按前两个加括号看待，或者按后两个加括号看待. 在第一种情况该表达式就好象 $(r\otimes s)\otimes t$，而在第二种情况则象 $r\otimes(s\otimes t)$. 因为 $\otimes$ 是我们集合上的一个二元运算，所以 $y=(r\otimes s)$ 和 $x=(s\otimes t)$ 都是我们集合上的元素. 因此 $(r\otimes s)\otimes t$ 和 $r\otimes(s\otimes t)$ 的每一个都可以作为仅涉及到这个集合的二个元素： 在第一种情况即 y 和 t；在第二种情况即 r 和 x.

若二元运算 $\otimes$ 是不可结合的，则元素 $r\otimes x$ 与 $y\otimes t$ 通常是不同的，从而表达式 $r\otimes s\otimes t$ 没有唯一的意义. 例如，在正

有理数集合上的除法这种情况下，表达式 $\frac{3}{2} \div 3 \div \frac{3}{4}$ 的含义就是模棱两可的，这是因为

$$\left(\frac{3}{2} \div 3\right) \div \frac{3}{4} = \frac{2}{3}, \text{而} \frac{3}{2} \div \left(3 \div \frac{3}{4}\right) = \frac{3}{8}.$$

如果二元运算⊗是可结合的，则元素 $r \otimes x$ 与 $y \otimes t$ 是相等的，所以我们所用的两种加括号方法并没有差别． 在这两种情况下，我们得到的都是同一元素的表示． 就是因为这种结合性，下面三个表达式

$$r \otimes s \otimes t,\ r \otimes (s \otimes t),\ (r \otimes s) \otimes t$$

显然也都是同一元素的表示．

公理 1（结合性公理） 在群中，一个二元运算是这样定义的：若 r，s 和 t 是任意三个元素，则

$$r \otimes (s \otimes t) = (r \otimes s) \otimes t.$$

用“接着”一词描述的运算是可结合的吗？ 为此，我们来考察一个象自行车轮子一样、能围绕通过它的中心的轴旋转的圆盘． 假设 a，b，c 是这个圆盘的旋转的任意集合，若用⊗表示“接着”运算（或旋转的相继），那么

$$(a \otimes b) \otimes c = a \otimes (b \otimes c)$$

总成立吗？ 容易看到，括号的用处仅仅在于破坏原有的那种 a 第一、b 第二、c 第三的次序． 对于旋转或其他运动的任意集合，这个运算是可结合的，从而是一个许可的群运算．

单位元素或么元

剩下的两个公理涉及到数 1 的概念的推广． 如果我们想到用通常的乘法作为我们的二元运算，那么这些公理似乎是

非常自然的．首先我们检查一下数 1 在乘法中的性质．若 n 是一个数，则

$$n \cdot 1 = 1 \cdot n = n;$$

这就是说，n 与 1 的乘积是 n． 将这个观点推广到群的元素和群的运算，我们得到公理 2.

公理 2（单位元素公理） 对任意的群元素 a，存在唯一的群的元素 I，使得

$$a \otimes I = I \otimes a = a.$$

在二元运算中，任意元素与元素 I 配对(作二元运算)都对应于它自己．这个元素 I 叫做群的单位元素或么元．之所以采用字母 I 作单位元素，是由于它与普通算术中的数 1 相象．

练习 3 假设集合是由实数组成的集合，而二元运算是加法，那么(群的)单位元素是什么元素？

倒数或逆元素

与推广数 1 有关的第二个概念，是将倒数概念推广到群．若 u 和 v 是任意两个使 $uv = 1$ 的数，则我们说 u 与 v 互为倒数．下面这个公理是这个观点的一个推广．

公理 3（逆元素公理） 若 a 是一个群的任意元素，则这个群存在唯一的元素 a^{-1}，使得

$$a \otimes a^{-1} = a^{-1} \otimes a = I.$$

元素 a^{-1} 叫做 a 的逆元素．显然 a^{-1} 的逆元素是 a：

$$(a^{-1})^{-1} = a.$$

之所以用a^{-1}作为a的逆元素的符号，是为了与普通代数相一致．在普通代数中，不等于0的u的倒数(即逆元素)是用u^{-1}表示的。

让我们来概括一下我们的群的定义．一个群是一个集合G及G上的一个二元运算$\otimes$，且使得如下的公理都成立：

公理1(结合性公理)　对G的任意元素r, s, t，都有

$$r\otimes(s\otimes t)=(r\otimes s)\otimes t.$$

公理2(单位元素公理)　对G的每一个元素r，在G中都存在唯一的元素I，使得

$$r\otimes I=I\otimes r=r.$$

公理3(逆元素公理)　对G的任意元素r，都存在G的唯一的元素r^{-1}，使得

$$r\otimes r^{-1}=r^{-1}\otimes r=I.$$

读者不应设想，这个群的公理化定义是从某一个数学家的头脑中一下子蹦出来的．数学概念常常是许多数学家以一种非常没有规律的方式发展起来的，一阵高一阵低，有时走到死胡同，有时却作出革命性的发现． 实际上构成群的基础的正式的公理，在群论工作中大约经一个世纪之久才表述清楚．

早在1771年拉格朗日(Lagrange)就已提出并证明了第一个重要的定理（在稍后一点的章节中我们将考虑这个定理）．但到1815年柯西●（Cauchy）开始写群论方面的著作时，考

● 奥古斯丁-路易斯・柯西，(1789—1857)，他强调数学分析的严格性而对数学的发展作出巨大贡献．他提出的"极限"，"连续性"及"收敛性"现在仍然是现代数学分析概念的基础． 柯西是使群论(特别是置换群论)得到系统发展的先驱者之一．他还以他的单复变函数论的基本定理而知名．

虑的还仅是元素是用置换表示的群. "群"这个词是伽罗华(Galois)在1832年引进的，伽罗华是第一个指出群可不用置换作元素来定义的人. 直到1854年，强调结构这种思想发展到使得凯莱[1](Cayley)才能指出，可不管元素种类的特殊性和具体性而抽象地定义群. 凯莱指出，群的本质结构仅依赖于规定元素对二元运算的方法.

在我们进一步给出群的一些例子之前，我们来简化并推广我们将利用的群的二元运算的符号. 初等代数的经验提醒我们，

$$a \otimes b = c$$

可简写成

$$ab = c,$$

读作：元素 a 乘元素 b 对应于元素 ab，ab 叫做 a 和 b 的**乘积**(也可记作 c). 今后，我们将不总是用 $\otimes$ 表示一般的二元运算，我们将用符号 ab 来表示 a 与 b 的**群乘法**. 有时我们也将 ab 写成 $a \cdot b$ 的形式.

用"乘法"作为群二元运算的一般术语，一般不会与普通算术中的乘法相混淆. 群的元素是数、群的二元运算是普通乘法的情况可以作为一个特殊情况出现. 但是在一般情况下，群的乘法将看作算术乘法的一种抽象推广.

注意 在一个集合的元素上虽然可以定义许多运算，但在任何特殊的群上，只有一个唯一确定的运算即群的运算.

---

[1] 亚瑟·凯莱(1821—1895)在数学的许多分支都有过著作，从几何和代数到理论动力学和物理天文学. 他同时花许多时间(用14年)从事法律工作. 现在凯莱主要以矩阵论上的创见及其在群论方面的工作而著名.

第三章 群 的 例 子

如果我们想要断定，具有特定二元运算的一个给定的元素集合是否构成一个群，我们必须逐一检查上述公理是否都能成立．让我们检查下面一些集合是否符合群的条件．我们首先由群A(见第2页)做起．

例 1

元素的集合 所有整数(正整数、负整数及0)．

二元运算 加法．

结合性 数的加法是可结合的．

单位元素 0是这个集合的一个元素，而且对每一个整数u都有$u+0=0+u=u$．所以0是单位元素．

逆元素 若u是一个整数,则$-u$也是一个整数,而且有$u+(-u)=(-u)+u=0$; 所以$-u$是u的逆元素．用群的记法即$u^{-1}=-u$．

所以,经过检验,这个集合是一个群．因为这个群有无限多个元素，所以我们称它是无限群，这个群有时也叫做无限加法群或整数加法群．

例 2

集合与例1相同,但现在改用乘法．读者自己不难验证，乘法是所有整数的集合上的二元运算，而且可结合性公理及单位元素公理都是成立的．现在来看这个集合是否满足公理3,我们来试求元素2的逆元素,为此我们需要一个能满足

$$2 \otimes u = I$$

即

$$2u = 1$$

的整数 u。这样的整数不存在，所以，改用乘法后就不是一个群。

例 3

集合由两个数 1 及 -1 组成，二元运算是乘法：

$$(1)(1) = 1; (-1)(-1) = 1;$$

$$(1)(-1) = (-1)(1) = -1.$$

结合性 无疑地。

单位元素 单位元素是 1。

逆元素 因为 $(1)(1) = 1$ 及 $(-1)(-1) = 1$，所以 $(1)^{-1} = 1$ 及 $(-1)^{-1} = -1$。 即每一个元素的逆元素是它自己。

所以我们得到一个群。 这个群的元素的个数是有限的，所以我们说它是有限群。一个有限群的阶就是集合的元素的个数。这个群的阶是 2。

例 4

有阶是 1 的群吗？用乘法作二元运算的仅含有数 1 的集合能作成一个群吗？对三个公理作检验即知，它是一个阶为 1 的群。

例 5

下面我们将考察一个群，它的元素是几何图形的运动。运动这个概念以后将经常出现，所以我们将详细叙述这个运动及运动群，以使读者有一个坚实的基础。

考察这样的运动：等边三角形在它所在的平面内绕过它的中心的轴所作的旋转。我们提到的群是以其中的某些特选的旋转作为元素的，而集合上的二元运算将是"接着"或"相继"（见第7页）。我们的兴趣在于，使三角形与它自己重合的那些运动，这样的运动叫重合运动。

为了给出重合运动的具体图形，我们首先在平面上任选一个特殊的位置作为等边三角形的（作任意旋转之前的）初始位置；其次在每一个顶点标示一个数作为识别的标记。可以如图3.1那样，中心的圆点表示旋转的轴与三角形所在平面的交点，而顶点的标记将帮助我们判别我们集合中的运动的不同。我们应当记住，三角形与它自己重合，并不是每一个（被标记）被分配的顶点都必须与它自己重合，而仅是三角形各边旋转之后必须与初始位置上的边重合。例如，如果图3.1中的三角形反时针方向绕轴转120°，我们能看到，旋转后的三角形好象是第二个三角形，它重叠于初始位置的三角形，如图3.2所示。图3.2中括号中的符号表示初始位置时的顶点。我们看

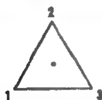


图 3.1

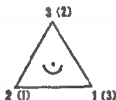


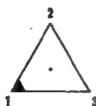
图 3.2

到，这种旋转伴随着顶点间的一个轮换：

1换成2，2换成3，3换成1。

为了简便起见，我们用象图3.3那样的方法来表示三角形的与它自己重合的两个位置。注意，顶点1的一角被涂黑将有助于识别三角形的运动。

有其他的旋转也能使三角形从原始位置进入上面画的第



初始位置



反时针转 120° 后的位置

图 3.3

二个位置吗？回答是肯定的，顺时针转 240° 是，反时针转 480° 或 840° 也是．读者可以自己验证，无限集合

$$A=\{\text{反时针转 }120° \pm (360k)°,\ k=0,1,2,\cdots\}$$

中的任意一个旋转都有同样效果（负的反时针旋转解释成一个顺时针旋转）.

集合 A 中的运动有一个共同性质，就是我们的三角形的顶点都用如下的特殊方式由初始位置变换为旋转后的位置：

初始位置		旋转后的位置
1	⟶	2
2	⟶	3
3	⟶	1

读者应注意，**集合的旋转所具有的这个性质与三角形的初始位置的选择无关**.

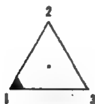
现在让我们取一个元素来表示集合 A 的任何一个元素．如下意义的顶点轮换(见图 3.4)：

$$a:\ 1\to 2,\ 2\to 3,\ 3\to 1$$

能够被看作是集合 A 的（三角形从任意选定的初始位置进入与它自己重合位置的）**代表元**．集合 A 的所有运动都有这个效果.

对于给出的位置，可以让 a 表示集 A 的某个特殊运动，例如(为了便于寻求) a 可以是反时针转 120°，这对应于在

$$120° \pm (360k)°$$



初始位置



运动 a 得到的结果位置

图 3.4

中选取 $k=0$. 如果读者愿意将 a 取作某个其他的特殊运动，例如他愿意取 $k=13$，则反时针转 $4800°$ 就是他所选取的集 A 的代表. 这种特殊的选取仅仅是为了方便. 重要的是，从集合 A 的所有运动，用同样方法选取我们的三角形的轮换顶点，都与它的初始位置无关. 我们可用

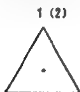


图 3.5

$$1\to 2,\ 2\to 3,\ 3\to 1$$

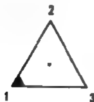
来标明我们的顶点轮换.

除此之外，集合 A 中还有其他的旋转(即三角形的重合运动)吗？考察旋转集合

$B=\{$反时针转 $240°\pm(360k)°,\ k=0,1,2,\cdots\}$.

这个集合的任何运动结果如图 3.5 所示. 图 3.6 则表示图 3.5 的"分开的"情况.

与上述类似，可用 b 表示集合 B 的任意一个元素，也就是



初始位置



b

图 3.6

作这个集合的一个"代表"。为了方便起见，我们用 b 标记这个运动的结果位置。这与从集合 B 选取的旋转无关，它的作用是三角形顶点的如下的轮换：

$$b: 1 \to 3,\ 3 \to 2,\ 2 \to 1$$

（也就是 1 变为 3，3 变为 2，2 变为1）。

三角形重合于它自身的旋转的其他集合是：

$C = \{$反时针转$0° \pm (360k)°,\ k = 0, 1, 2, \cdots\}$.



图 3.7

在图 3.7 中，c 是集合 C 的任意元素。注意，运动 c 是三角形回到原始位置的旋转，其效果是如下的顶点对应：

$$c: 1 \to 1,\ 2 \to 2,\ 3 \to 3.$$

我们的目的是要得到一个运动群；由于一个群必须含有一个单位元素(单位元素公理)，所以我们将注意辨认集合 C 的任意运动 c 是否可作为一个单位元素。事实上，若 x 是集 A，B 或 C 的任意元素，则"x 接着 c"是一个与 x 处于同一集合的旋转，而且"c 接着 x"也是一个与 x 处于相同集合的旋转。为了看出这一点，我们应回想起，A 中的旋转是旋转

$$120° \pm (360k)°,\ k = 0, 1, 2, \cdots,$$

而 C 中的旋转是旋转

$$0° \pm (360m)°,\ m = 0, 1, 2, \cdots.$$

如果一个旋转后接着又一个旋转，则旋转的角度将是这两个旋转角度的和。所以"a 接着 c"旋转的角度是

$$120^\circ \pm (360k)^\circ + 0^\circ \pm (360m)^\circ$$

即

$$120^\circ \pm (360(k+m))^\circ.$$

因为 k 和 m 是整数，所以 $k+m$ 是整数，所以旋转"a 接着 c"在集 A 内。类似地，"c 接着 a"是旋转

$$120^\circ \pm 360(m+k)^\circ,$$

也在 A 内。

应用群乘法(第 13 页)的概念，我们有

$$ac = ca = a,\ bc = cb = b,\ cc = c,$$

这些结果是普遍有效的，与集合 A、B 和 C 的元素（分别表示为 a，b 及 c）的选取无关。这些结果证明，集合 C 中的任意元素可用符号 I（表示单位元素）代替。

我们详细讨论了所有绕轴的重合旋转。三个集合 A、B、



图 3.8

C 包含了每一种旋转。这三个集合的代表元 a、b、I 的"分开的"位置如图 3.8 所示。注意三角形的三个位置中的每一个，都是三角形从初始位置到描述位置的运动的符号表示。我们认为，包含重合运动三个类(分别以 I，a，b 为代表元)的集合作成的群是用"接着"作为二元运算的。为了验证"接着"是这个集合上的二元运算，为了验证群公理，我们需要求出两个元素的所有乘积。例如，让我们应用顶点对应的办法并按运动"a 接着 b"的含义来求 ab。

$$a: \; 1 \to 2 \qquad b: \; 1 \to 3$$
$$2 \to 3 \qquad 3 \to 2$$
$$3 \to 1 \qquad 2 \to 1$$

运动 a 将顶点 1 变为顶点 2；运动 b 又将顶点 2 变到顶点 1；所以运动 a 之后接着运动 b 的效果等于将顶点 1 变到它自己．类似地，a 将 2 变到 3，b 将 3 变到 2，所以 ab 将 2 变到它自己，如此等等．所以有

$$ab: \; 1 \to 2 \to 1, \quad 即 \quad 1 \to 1,$$
$$2 \to 3 \to 2, \quad 即 \quad 2 \to 2,$$
$$3 \to 1 \to 3, \quad 即 \quad 3 \to 3.$$

显然有

$$ab = I.$$

读者容易验证，其余的乘积是

$$aa = b, \; bb = a, \; ba = I.$$

现在我们已肯定了"接着"是我们集合上的二元运算．我们剩下的仅需验证群公理也是满足的．

结合性 我们在 10 页已经指出，当集合的元素是运动时，相继运算是结合的．

单位元素 上面的讨论已经指出，集合 C 的代表元 I 是单位元素．

逆元素 因为

$$ab = I, \; ba = I \text{ (当然还有 } I \cdot I = I),$$

所以每一个元素在这个集合中都有一个逆元素．

例 6

假设对任意的整数，我们仅考虑它除以 2 的余数，而且若两个整数有相同的余数，则我们说它们是相等的．这样一来，两个都是偶数的整数是相等的，都是奇数的也是相等的．我

们用

$$8 \equiv 6 \pmod 2$$

表示：当除以 2 时，8 与 6 有相同的余数，其中“$\equiv$”表示“相等”，而“mod”是“模”这个字的英文“modulo”的缩写．类似地我们能写

$$7 \equiv 3 \pmod 2,$$

这是因为 7 与 3 除以 2 时有相同的余数．所以，如果 x 表示任意的偶数，而 y 表示任意的奇数，则我们可以记为

$$x \equiv 0 \pmod 2, \quad y \equiv 1 \pmod 2.$$

事实上，这个“模 2 相等”的概念使我们能够用 0 和 1 分别“表示”偶数和奇数．

现在我们来检验用“模 2 加法”作二元运算且仅有 0 与 1 两个元素的集合能否作成一个群．为此，我们先如下地定义两个整数 a 与 b 的模 2 加法(用$\oplus$表示)：若

$$a + b \equiv 0 \pmod 2,$$

(即如果 a 与 b 的通常的和是偶数)，则

$$a \oplus b = 0;$$

若

$$a + b \equiv 1 \pmod 2,$$

则

$$a \oplus b = 1.$$

模 2 加法是集合 $\{0, 1\}$ 上的一个完全确定的二元运算，这是因为

$$0 + 0 \equiv 0 \pmod 2, \quad 0 + 1 \equiv 1 \pmod 2,$$
$$1 + 0 \equiv 1 \pmod 2, \quad 1 + 1 \equiv 0 \pmod 2,$$

即

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1, \quad 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0.$$

结合性 检验模 2 加法是可结合的是容易的，例如

$$1+(1+1)\equiv 1+0\equiv 1 \pmod 2,$$

$$(1+1)+1\equiv 0+1\equiv 1 \pmod 2.$$

单位元素 0 是单位元素.

逆元素 因为

$$0+0\equiv 0 \pmod 2,\quad 1+1\equiv 0 \pmod 2,$$

所以每一个元素的逆元素是它自己.

我们恰好把所有的整数划分为两类，偶整数用 0 表示，奇整数用 1 表示. 当我们考虑除以 3 的余数时，也可以把所有的整数集合划分成 3 类：所有除以 3 余数为 0 的整数是一类，所有余数为 1 的是另一类，所有余数为 2 的是第三类. 我们有，例如

$$12\equiv 15 \pmod 3,\quad 7\equiv 1 \pmod 3,\quad 5\equiv 8 \pmod 3;$$

也就是说，除以 3 后余数相同的整数是模 3 相等的.

类似地，按除以 4 的余数，我们可以考虑整数模 4 的等价类，一般地，可考虑模任意整数 n 的整数等价类. 因为除以 n 时所有可能的余数是

$$0,\ 1,\ \cdots,\ n-1,$$

所以我们得到 n 个等价类，我们可用 $0,\ 1,\cdots,\ n-1$ 表示这些等价类.

读者自己验证，有二元运算"模 n 加法"的集合

$$\{0,\ 1,\ 2,\ \cdots,\ n-1\}$$

构成一个群.（若 x 是我们集合的任意元素，它的逆元素是什么？我们求满足

$$x+y\equiv 0 \pmod n$$

的元素 y 时，应注意 $n\equiv 0 \pmod n$.）

例 7

现在我们来考察有二元运算"模 5 乘法"的整数集 $\{1, 2, 3, 4\}$. 所谓"模 5 乘法"是指,对任意两个整数 r 及 s,若

$$r \cdot s \equiv t \pmod 5,$$

也就是如果除以 5 时 $r \cdot s$ 与 t 有相同的余数,则记作

$$r \otimes s = t \text{ 或 } (r, s) \to t.$$

例如,因为 $3 \cdot 4 = 12 \equiv 2 \pmod 5$, 所以

$$3 \otimes 4 = 2 \text{ 或 } (3, 4) \to 2.$$

如证明出任意两个元素的乘积都等于我们集合中的某一个整数时,读者也就验证了模 5 乘法是我们集合上的二元运算.

结合性 由整数的普通乘法的可结合性推得模 5 乘的可结合性(验证这一点).

单位元素 单位元素是 1.

逆元素 1的逆元素是它自身; 2, 3 及 4 的逆元素由如下的关系式推得:

$$2 \cdot 3 \equiv 1 \pmod 5), \ \therefore 2 \text{ 的逆元素是 } 3;$$

$$3 \cdot 2 \equiv 1 \pmod 5), \ \therefore 3 \text{ 的逆元素是 } 2;$$

$$4 \cdot 4 \equiv 1 \pmod 5), \ \therefore 4 \text{ 的逆元素是 } 4.$$

试问从我们的集合中去掉 0 是必须的吗? 也就是说, 在模 5 乘法这个运算下,集合 $\{0, 1, 2, 3, 4\}$ 是一个群吗?

读者还可以提这样的问题: 集合 $\{1, 2, 3\}$ 在模 4 乘法这个二元运算下构成一个群吗? 读者首先应试求 2 的逆元,也就是求适合

$$2x \equiv 1 \pmod 4$$

的元素 x.

例 8

一个大于 1 的整数, 如果它只有 1 及自身这两个正整数

因子，则说它是一个素数．设 p 是一个素数，考察集合

$$\{1, 2, 3, \cdots, p-1\}.$$

我们指出，"模 p 乘法"是这个集合上的一个二元运算，而且群的三个公理都成立．读者可以假设结合性公理及单位元素公理是成立的，作为练习的仅是：证明逆元素公理也是成立的．

练习 4　p 是一个素数，考察有二元运算"模 p 乘法"的集合 $\{1, 2, 3, \cdots, p-1\}$．证明对这个集合的任意元素 x，在这个集合中都存在一个元素 y 使得

$$xy \equiv 1 (\bmod p).$$

第四章　群的乘法表

现在我们必须着手考虑这样的问题：我们怎样才能确定一个特殊的群？换句话说，在数学上要多少信息量才足以确定一个群？而我们又将怎样显示确定一个特殊群的数据？

凯莱（Cayley）在1854年引进了群的乘法表，从而给出了这些问题的回答。这种乘法表的排列形式类似于熟知的算术中的乘法表。群的元素排在表的最上一行，并以同样的次序排列在表的最左边一列，而表中的值则是群元素的乘积。

首先考察阶为2的、仅包含两个元素1及−1的、用普通乘法作二元运算的群。表4.1展示了这个群的两个元素的所有可能的乘积。因为普通乘法是可交换的，所以这个群的任意两个元素可以相互交换。

	1	−1
1	1	−1
−1	−1	1

表　4.1

其次我们将构造等边三角形的在平面中的重合旋转的群（见例5，第15页）的乘法表。当用I，a，b表示这个群的三个元素时，我们将它们及它们的乘积排列成表4.2。这里的解释和简化应按次序，所以我们不能随便将这个群的任意两个元素相互交换。由于这个原因，乘积中的每一个因子是按执行乘法时的次序写的，列表时还规定将第一个因子排在表的最左边一列，第二个因子排在表的最上面一行。

我们曾详细讨论过这个群，在第21页我们还求得

$$aa=b,\ ab=ba=I,\ bb=a.$$

第二个因子

第一个因子	I	a	b
I	$I \cdot I$	Ia	Ib
a	aI	aa	ab
b	bI	ba	bb

表 4.2

当利用这些结果及单位元素 I 的一些性质时，我们可以将这个乘法表写成如表 4.3 所示.

第二个因子

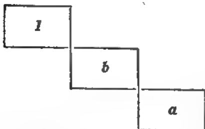
第一个因子	I	a	b
I	I	a	b
a	a	b	I
b	b	I	a

表 4.3

这个旋转群的许多性质可以从它的乘法表上直接看出. 逆元素可以在表中出现 I 的行和列观察到. 注意表中还有如下有趣的"一致性"：每一行是最上面一行的重新排列(或置换)，每一列是最左边一列的重新排列.

这个乘法表还表明，这个群的所有的元素都是可以互相交换的，这是由关于主对角线对称的各元素的乘积都相同这一点看出的. 所谓主对角线，就是从表的左上角到右下角的线，表 4.3 中的主对角线是





在任何乘法表中，如果一个乘积是 rs，则与其对称的元素的乘积就是 sr. 如果一个群的任意两个元素都是可交换的，则称这个群是交换群. 因此我们可以说：

一个有限群是交换群，当且仅当它的乘法表中关于主对角线对称的各元素的乘积都是相同的群元素.

一个等边三角形的重合旋转群的其他重要性质，从这个乘法表的当前形式还不能直接看出，但是以后我们将引进某个新记法，并应用它将这个乘法表写成其他更明显的形式.

由于群乘法是普通乘法的一种推广，所以我们也可以将群元素 aa 用 a^2 表示，aaa 用 a^3 表示，一般地，k 个 a 的乘积用 a^k 表示. 类似地，$(a^{-1})(a^{-1})$ 可以写成 a^{-2}，k 个 a^{-1} 的乘积可以写成 a^{-k}. 由于

$$a^k \cdot a^{-k} = I,$$

所以很自然地定义 $a^0 = I$. 群元素 a^n 叫做 a 的 n 次方，其中 n 是任意整数. 读者自己可以验证，对乘幂的通常规则对于群乘幂也成立.

前面讨论这个群时曾得到

$$b = aa = a^2,$$

$$ab = aaa = a^3 = I,$$

所以这个群的乘法表可以写成表 4.4 的形式. 在最后这种形式中看到，这个群的每一个元素都是元素 a 的方幂. 具有这种性质的群叫做是由 a 生成的群，a 叫做生成元. 这一概念将在稍后的讲群的生成元的那一节进一步讨论.

	I	[illegible]	a^2
I	I	a	a^2
a	a	a^2	I
a^2	a^2	I	a

表 4.4

非交换群

虽然我们遇到过非交换元素对的例子，但我们还没有见过非交换群．前面讲到交换群时是作为其任何两个元素都可交换来定义的．这样的群又叫阿贝尔群．采用这个名称是为了纪念数学家阿贝尔● (Abel) 的工作，他是第一个将这样的群应用于方程理论的人．

一个群只要有两个元素不可交换，这个群就叫做非交换群；就是说，在非交换群中可以有一些元素对是可交换的．能找到任何两个元素都不可交换的群吗？回答是明确的"不能"．原因很简单：每一个群都必须含有单位元素 I，而 I 与每一个元素都可交换．

现在让我们来构造一个阶为 6 的非交换群．以后我们将看到，对非交换群来说，这已是最小的可能的阶．为了构造我们的群，我们来考察等边三角形的使它与其自身重合的旋转．我们曾限制三角形只能在它所在的平面内旋转，并检验了这种旋转的集合，看到它们构成一个阶为 3 的群．如果我们取消这种限制，则还有其他旋转也是所容许的．这是因为三角

● 挪威数学家 N. H. 阿贝尔证明了：一般的五次代数方程不可能用根式求解．在他的代数方程的工作中，他应用了交换群(现在叫"阿贝尔群")的概念．他还在函数论(特别是椭圆函数)的探讨中打开了新的领域．他死于结核病时年仅 26 岁．

形还能越出平面作转动——翻转．例如，以它的一个高为轴翻转三角形时，也可使它与自己重合，但这并不是例 5（第 15 页）中研究过的旋转．我们将看到，现在三角形与它自己重合的位置共有 6 个．我们用

$$I, r, r^2, f, fr, fr^2$$

分别标记这 6 个位置(见图 4.1)．

为了引起读者对空间有直观感觉，在本书中将时常有群

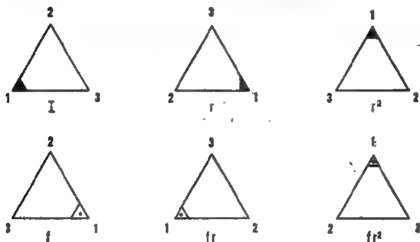


图 4.1

性质的几何表示．我们建议读者最好采用物理模型作辅助．例如，在这里若用纸板剪下等边三角形以模仿所说的旋转，将有助于把运动形象化．

为了构造我们的群，下面我们利用与例 5（15 页)类似的方法．用这种方法对付旋转群是比较方便的．

用来表示运动的符号常常给一个特殊的意义．在这一节，r 表示等边三角形的绕过中心的轴反时针转 120°，但它也可以表示集合 A 的任意一个反时针旋转

$$120° \pm (360k)°, k = 0, 1, 2, \cdots$$

的元素. 类似地，稍后，我们也将引进运动 f，为了便于运动形象化也给它一个特殊的意义，即用它来表示三角形的“翻转”运动. 重要的是，我们将把所有这些用同样方法作的顶点对应作为同样的运动来考虑.

我们希望，我们的群的运动有一个图形表示，但本书的静止图形不能直接描绘运动.因此，我们将采用 20 页的办法：用一个静止的图形来作为一个运动的表示，也就是，如果符号 x 表示一个指出图形的位置，则我们将把这个图形理解为从所给的原始位置到标记位置 x 的运动的一个表示.

随后，我们将发现，用 r 表示绕垂直于三角形所在平面且过三角形中心的轴、反时针转 120° 的旋转将是方便的. 于是，正如我们已经看到的，运动 I, r, r^2 只能到达前三个位置(我们应回想起，I 是转 $0° \pm (360k)°$ 的旋转).

为了到达其余的新位置，我们必须设法翻转这个三角形. 我们能用三角形绕过一个顶点的高转 180° 的旋转来实现这一点. 我们选过顶点 2 的高作为我们的旋转的轴. 我们用 f 表示绕这个轴转 180° 的旋转. 当然，f 也可以表示绕这个轴转

$$180° \pm (360k)°$$

的任意一个旋转. 所以我们有图 4.2 中的图形.

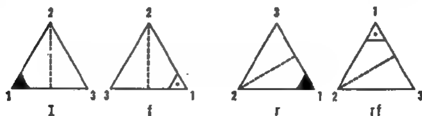


图 4.2

我们将试图阐明符号 fr 的意义．为此我们将图 4.1 中用 f 和 fr 标记的位置在图 4.3 中又重画了一下．由图 4.3 看到，旋转 r 似乎是顺时针转 120°，而不是所述的反时针转 120°．但是如果我们注意到翻转三角形时旋转 r 的轴也被翻转（因而旋转方向就相反)的话，这种表面上的矛盾也就不存在了．首先我们需要对旋转 r 作更详细的叙述．我们取通过三角形中心的垂直于它所在平面的直线为轴，这个轴的方向如图 4.4 中的箭头所示，而我们的旋转 r 则伴随着如下的顶点轮换：

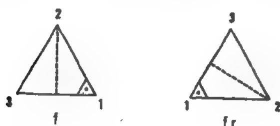


图 4.3

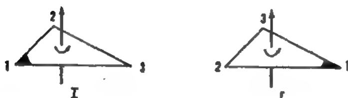


图 4.4

$$1 \to 2,\ 2 \to 3,\ 3 \to 1$$

(也就是 1 变为 2，2 变为 3，3 变为 1)．

现在我们设想，轴的箭头是右旋螺钉的旋进方向，旋转 r（三角形转 120°）的效果相当于你将右旋螺钉旋紧． 如果图 4.4 中的第一个三角形被 f 翻转，则它将变成图 4.5 中 f 所标记的位置． 注意，轴的箭头已因翻转而倒过来了． 如果后来这个三角形接着旋转 r（旋转 r 使右旋螺钉旋紧)，则得到的

位置就是图 4.5 中 fr 所标记的位置. 所以，不管三角形是处于位置 I 还是处于 f 所标记的位置，旋转 r 都与如下的顶点轮换相同:

$$1\rightarrow 2,\ 2\rightarrow 3,\ 3\rightarrow 1.$$

以三角形的 6 个可能位置作为图示的运动的 6 个类组成的集合，以相继或"接着"作二元运算，就作成一个群. 我们已经知道，运算是相继，单位元素 I 是这个集合的一个元素，(在这个基础上) 逆元素公理的成立也可直观地看出，这是因为，如果有一个运动将一个位置变为另一个，则反转过来的变换(逆变换)就变回原来位置.

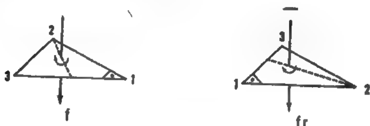


图 4.5

第二个因子

第一个因子	I	r	r^2	f	fr	fr^2
I	I	r	r^2	f	fr	fr^2
r	r	r^2	I	rf	rfr	rfr^2
r^2	r^2	I	r	r^2f	r^2fr	r^2fr^2
f	f	fr	fr^2	I	r	r^2
fr	fr	fr^2	f	frf	$frfr$	$frfr^2$
fr^2	fr^2	f	fr	fr^2f	fr^2fr	fr^2fr^2

表 4.5

借助于乘法表来显示某些群的性质将是有启发性的．注意，按 r，f，I 的意义即有

$$r^3 = I，\ f^2 = I．$$

利用这些特殊性质我们就可构造出表 4.5．

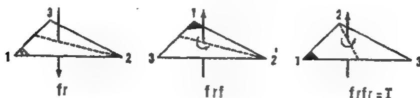


图 4.6

为了完全造出我们群的乘法表，我们必须将表 4.5 中的每一格都表示成 6 个元素

$$I，r，r^2，f，fr，fr^2$$

中的一个．我们仔细地化简其中的两个乘积，而把其他的留给读者．首先我们证明 $frfr = I$．为此我们考察图 4.6 中的一系列图形．其第一个表示 fr．三角形从这个位置开始，绕过顶点 2 的高翻转 180°，其结果 frf（fr"接着"f）如第二个图形所示．然后我们绕过中心的轴沿右旋螺钉的旋进方向转 120°，其结果，$frfr$，如最后一个图形所示；我们看到，它与用 I 标记的初始位置相同．所以有 $frfr = I$．

其次按图 4.7 中的图形的意义，可以证明 $rfr^2 = fr$．

利用所有这样化简的乘积，我们作成乘法表 4.6．这个表



图 4.7

揭示了:

(1)"接着"是我们的所有元素的二元运算,

(2)因为 I 在每一行每一列出现,所以逆元素公理是满足的.(而且由这个表)我们能立即确定任意一个群元素的逆元素. 例如,由如下的相对位置



就得到 $(fr)^{-1}=fr$.

第二个因子

第一个因子	I	r	r^2	f	fr	fr^2
I	I	r	r^2	f	fr	fr^2
r	r	r^2	I	fr^2	f	fr
r^2	r^2	I	r	fr	fr^2	f
f	f	fr	fr^2	I	r	r^2
fr	fr	fr^2	f	r^2	I	r
fr^2	fr^2	f	fr	r	r^2	I

表 4.6

(3)这个群是非交换的. 这由关于主对角线处于对称位置的元素一眼就看出了,例如

$$(fr)f=r^2\neq r=f(fr).$$

(4)表的每一行及每一列分别是最上面一行及最左边一列的元素的置换(或重新排列),这种"重合性"是以前就观察到的.

(5) 左上角的 3×3 方阵正是等边三角形在平面上的旋转的三阶群的乘法表. 在主对角线的下部，在右下角有一个 3×3 方阵，它是左上角方阵的重新排列. 但是在左下角和右上角有两个主对角线方阵，它们是用每一个乘积加一个前缀 f 得到的. 如果用 M 表示左上角 3×3 方阵的元素的集合，则表 4.7 用符号表示了这个乘法表的范型中的范型，这给我们提供一个暗示，以帮助我们进一步分析群的结构. 我们将在稍后的关于正规子群和商群的章节中探讨这些可能性.

M	fM
fM	M

表 4.7

群的乘法表的结构

现在我们来察看群的乘法表的内部结构. 首先我们检验上面的(4)中叙述的"重合性"，也就是检验群乘法表中的行和列分别是最上面的行及最左边的列的置换. 我们将证明，这并非是一种巧合，它是群的乘法表的一个特征性质. 证明这一点之后，我们将把一个群的乘法表看成由一列符号排成一个方阵的范型. 在这个阵列中我们将看到符号的空间范型，并指明它们如何对应群的关系. 由此可见，一个群的结构反映在它的乘法表的"几何"性质中. 可以证明，反之，有这些"几何"性质的方阵是一个群的乘法表.

"解"群的"方程". 在谈及群元素和它的关系时，有时必须能够回答这样一个问题：如果 a 和 b 是群的两个已知元素，这个群是否存在一个元素 x，使得 $ax = b$? 我们断言，$x = a^{-1}b$ 是我们要求的群元素，这是因为

$$a(a^{-1}b) = (aa^{-1})b = Ib = b;$$

所以 $x = a^{-1}b$ 满足群"方程" $ax = b$.

有其他可能的解吗？为了回答这个问题，我们来证明：只要 y 是 $a\ x = b$ 的解，就有 $y = a^{-1}b$；换句话说，$a^{-1}b$ 是唯一解. 首先我们设有一个群元素 y 使得

$$ay = b;$$

根据逆元素公理，又知道 a^{-1} 存在，所以我们能在 $ay = b$ 的两边同时左乘 a^{-1} 得

$$a^{-1}(ay) = a^{-1}(b),$$

因而有

$$(a^{-1}a)y = a^{-1}b, \quad \text{（根据结合性公理）}$$

$$Iy = a^{-1}b,$$

$$y = a^{-1}b. \quad \text{（根据单位元素公理）}$$

因为我们已经验证过，用元素 $a^{-1}b$ 替换 y 满足群方程，于是 $a^{-1}b$ 是唯一解得到证明.

注意，在这个证明中，所有的群公理都是需要用上的.

形如

$$xa = b$$

的群方程的解也可类似地讨论（其中 a 和 b 都是群元素）：在两边同时右乘 a^{-1}，我们就得解

$$xaa^{-1} = x = ba^{-1}.$$

将我们的结果公式化后可作为"规则"：

为了"解" $ax = b$，左乘 a^{-1}，求得 $x = a^{-1}b$；

为了"解" $xa = b$，右乘 a^{-1}，求得 $x = ba^{-1}$.

练习 5 对如下的每一个群方程，求解 x：

(a) $abx = c$, (b) $axb = c$,

(c) $xab = c$, (d) $a = bx^2$ 和 $x^3 = I$,

(e) $x^3 = a$ 和 $x^4 = I$, (f) $x^{-1} = abc$.

作为当前讨论的第一个应用，我们将证明一个关于群元素和它们的逆元素的关系(这个关系后面要用到)．假设我们有一个群元素表示成其他群元素的乘积，例如

$$d = ab,$$

问题是：我们能将 d 的逆元素 d^{-1} 表示成什么？一个与之等价的问题是：我们能求一个什么样的群元素 x，使得

$$dx = I? \text{ 或 } abx = I?$$

我们从前面的讨论知道，群方程有唯一解，为了求这个解，我们首先左乘 a^{-1} 得到

$$a^{-1}abx = a^{-1}I,$$
$$bx = a^{-1},$$

然后再左乘 b^{-1} 得到

$$b^{-1}bx = b^{-1}a^{-1},$$
$$x = b^{-1}a^{-1}.$$

为了验证 $d^{-1} = b^{-1}a^{-1}$，我们只需证明 $d(b^{-1}a^{-1}) = I$ 即可：

$$\begin{aligned} d(b^{-1}a^{-1}) &= ab(b^{-1}a^{-1}) = a(bb^{-1}a^{-1}) \\ &= a[(bb^{-1})a^{-1}] = aa^{-1} \\ &= I. \end{aligned}$$

类似地，如果 $d = abc$，则 $d^{-1} = c^{-1}b^{-1}a^{-1}$．范型是清楚的，因而我们能得出一般命题：若

$$d = a_1a_2\cdots a_n,$$

则

$$d^{-1} = a_n^{-1}a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1}.$$

换句话说，**乘积的逆元素是按照相反次序的逆元素乘积**．

作为群方程解法的一个附带应用，我们将证明一个定理，它解释为什么群的乘法表的任意的行(或列)是其他行(或列)的元素的重新排列．

我们假设有一个由元素

$$a_1, a_2, \cdots, a_n$$

组成的 n 阶群(当然，这些元素中必有一个是单位元素 I，但是它没有被特殊地标记出来)．取这 n 个元素中的任意一个，例如 a_i，为了方便，把它叫做 b． n 个元素左乘 b 的乘积是

$$ba_1, ba_2, \cdots, ba_n.$$

那么这些乘积是原来的 n 个群元素，可能是它们的重新排列．为了证明这一点，我们将指出，这些乘积中没有任何两个能够是同一个群的元素．假设，例如

$$ba_i = ba_j, \text{（其中 } i \neq j\text{），}$$

则左乘 b^{-1} 时得到

$$b^{-1}ba_i = b^{-1}ba_j,$$

即

$$a_i = a_j, \ (i \neq j).$$

但是如果 $i \neq j$，a_i 与 a_j 是不同的群元素，与假设 $ba_i = ba_j$ 发生矛盾．因此这 n 个乘积都是不同的．因为这些不同的乘积的每一个都是原来群的一个元素，它们合在一起必然是所有 n 个群元素．证毕．

以上我们是用左乘来证明的．右乘群的元素也有类似结果．对有限群我们就完全证明了：

定理 1 若 $a_1, a_2, \cdots, a_n$ 是 n 阶群的不同元素，且若 b 是这个群的任意一个固定的元素（当然 b 必须是这 n 个元素中的一个)，则乘积

$$ba_1, ba_2, \cdots, ba_n \text{（或 } a_1b, a_2b, \cdots, a_nb\text{）}$$

由所有 n 个群元素组成，可以是它们的重新排列(当 $b \neq I$ 时是重新排列)．

这个定理保证了，群乘法表的每一行和每一列都分别是

最上面一行和最左边一列的元素组成的，只是重新排列一下.

下面将对乘法表的性质作一简要介绍，其目的在于指出，一方面群的公理和它的一些推论将用来确定乘法表中的关于符号的空间关系的范型，另一方面展示这些范型的方阵是一个群的乘法表. 由于这些特殊概念并不是后面几章的主要部分，所以即使这个简短的解释在第一次阅读时不完全精通，也不影响后面内容的理解.

假设我们有一个组成方阵的符号集合，也就是群的乘法表，那么这个方阵有如下五个性质（至于这些性质的具体体现，读者可参照35页的6阶群的乘法表）：

(1) 方阵恰好包含和行(或列)一样多的不同符号；所以方阵如果有 n 行和 n 列，则组成这个方阵的 n^2 个符号中恰好有 n 个不同的符号. 方阵的这个性质反映了这样一个事实，即群是一个由 n 个元素组成的、有二元运算的集合.

(2) 每一个符号在每行和每列中恰好只出现一次. 这反映了定理1断定的事实.

(3) 假设表示群的所有不同符号被排列成某个确定的次序，而且群的乘法表的行和列也是根据这个次序标记的. 例如，我们可以有有序符号

$$a, b, I, c, \cdots, k.$$

我们知道，符号 I 因为是单位元素，所以它必然在这种有序符号中出现（在我们的例子中，我们是将它作为第三个元素）. 对应于群的单位元素公理，我们有方阵的第三个性质：方阵中被符号 I 标记的一行与方阵的最上面的一行的符号完全相同；被符号 I 标记的一列与方阵的最左边的一列的符号完全相同. 这个性质已用表4.8加以说明.

(4) 关于存在逆元素的群公理确定方阵这样的性质：

方阵中的每一个符号都伴随着另一个符号，使得标记第一个符号(例如 r) 的行与标记第二个符号(例如 s) 的列的交点处的符号是 I；标记 s 的行与标记 r 的列的交点处也是 I；而且这两个 I 是关于主对角线对称的．这个范型(见表 4.9) 反映了

	a	b	I	c	$\dots$	k
a			a			
b			b			
I	a	b	I	c	$\dots$	k
c			c			
$\cdot$			$\cdot$			
$\cdot$			$\cdot$			
$\cdot$			$\cdot$			
k			k			

表 4.8

$$rs = sr = I$$

(即 s 是 r 的逆元素)这个事实.

(5) 结合律对应于方阵的如下性质：方阵就是群的乘法表．假设我们在方阵中选择任意两个符号 r 和 s，使得包含 r 的列与包含 s 的行的交点是出现 I 的地方．这个包含 r 的列用某个群元素(例如 y) 打头，包含 r 的行用一个元素 u 标记在最左边．类似地，包含 s 的列由 x 打头，包含 s 的行用 v 标记(见表 4.10)．由结合律知，包含 r 的行与包含 s 的列的交点，也就是乘积 ux 处，必须是 rs．为了看出这一点，我们应看到(见表 4.10)

	r	s
r		I
s	I	

表 4.9

	x	y
u	ux	r
v	s	I

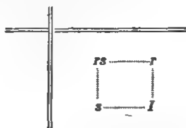
表 4.10

$$vy = yv = I,\quad uy = r,\quad vx = s,$$

所以

$$ux = uIx = u(yv)x = (uy)(vx) = rs.$$

所以乘法表必须体现这样的范型:



练习 6 在作为一个群乘法表的方阵中，如下"矩形"



的四个顶点中未定出的顶点必须是什么群乘积?

为了结束群乘法表的讨论，我们回到这一章一开始提出的问题：确定作为一个数学实体的群，需要多少信息量?我们又怎样指示这些数据?这些问题的回答是：对于 n 阶有限群，我们需 n^2 个信息单位，也就是这些群元素的所有可能的二元乘积．在我们的群乘法表的方阵中指示了这 n^2 个乘积．一个方阵表示一个群，当且仅当这个方阵中的符号都满足上面五个"几何"性质．

练习 7 构造元素为

$$1,\ 2,\ 3,\ 4$$

的、二元运算为"模 5 乘法"的群的乘法表(参考 24 页关于这个"剩余类"群的讨论)．

第五章　群的生成元

虽然群的乘法表能隐含地告诉我们，只要任何两个群元素的乘积规定好，就能知道我们所要了解的群的一切性质，但我们也能预见到，当企图无限扩大它的应用范围时，也会遇到某些困难．例如，不难设想，企图借助乘法表来分析一个阶为60的群就有实际限制．

现在我们转向生成元概念．这个概念是另一个刻划群的途径，在某种意义上，它与群的阶无关．本书的一个首要目标是群的图象表示，群的生成元概念是实现这一目标的一个重要环节．

假设 a 和 b 是群的元素，则按逆元素公理 a^{-1} 及 b^{-1} 也是这个群的元素，从而

$$ab^{-1}a,\ aba^{-1}b,\ \cdots$$

也是群元素．能用

$$a,\ b,\ a^{-1} \text{ 及 } b^{-1}$$

作为因子的每一个乘积，不管其顺序及出现的次数的多少，按二元运算的定义，都是这个群的一个元素．若这个群的所有的元素都能表成仅含 a 及 b（以及它们的逆元素）的乘积，则我们称 a 及 b 是这个群的生成元．我们能把群生成元这个概念推广到多于两个群元素的一个集合．若 S 是群 G 的元素的一个集合：

$$S=\{a,\ b,\ c,\ \cdots\},$$

而且如果 G 的所有元素都能表示成仅含 S 的元素（及它们的逆元素）的乘积，则我们称 S 的元素叫做 G 的生成元．

最简单的情况是只有一个生成元(例如 a)的群；这个群的所有元素都能表示成仅含 a 及其逆元素 a^{-1} 的因子的乘积. 我们已经见过一个生成元的群：以表 5.1 作为乘法表(见 27 页)

	I	a	a^2
I	I	a	a^2
a	a	a^2	I
a^2	a^2	I	a

表 5.1

的群，即正三角形在所在平面的旋转群. 因为

$$I = aa^{-1},$$

所以 3 个群元素 I, a, a^2 的每一个显然都是仅以生成元 a 或 a^{-1} 作为因子的乘积.

循环群

为了显示三角形旋转群的本质特征，我们指出，由于 $a^3 = I$，所以生成元 a 的乘幂序列

$$a, a^2, a^3, a^4, a^5, a^6, a^7, \cdots$$

可以写成

$$a, a^2, I, a, a^2, I, a, \cdots.$$

这里我们看到有一个以

$$a, a^2, I$$

为基本范型的**循环**重复. 由于这个原因，这个群被称为**阶为 3 的循环群**.

我们可以类似地定义任意阶的循环群：若一个群的每一个元素都成表示成某个生成元 a 的幂次，则这个群叫做**循环群**. 我们将用 C 作为表示循环群的一般符号，而群的阶则用

下标来表示．例如，C_3表示阶为3的循环群，而C_n就表示阶为n的循环群．

若n是使

$$a^n = I$$

的最小整指数，则由a生成的群将是n阶的．这个使得$a^n = I$的最小的整指数也叫做元素a的周期．例如，在上面叙述过的循环群C_3中有

$$a^6 = I,\ a^9 = I,\ a^{-3} = I,\ \cdots,$$

但还有$a^3 = I$，而且这个3是使

$$a^n = I$$

成立的最小的整指数，所以我们说元素a的周期是3．

若a生成一个循环群C_n，则a的逐次递增的乘幂序列能构成一个以

$$a,\ a^2,\ \cdots,\ a^n \quad (a^n = I)$$

为基本范型的循环重复序列．用这个特征（对群）作几何解释（即用它来作群的图象表示）是很适合的．例如，阶为3的循环群使我们联想到一个三角形，这个三角形的每一个顶点都对应于一个群元素（见图5.1）．这个三角形的每一边有一个箭头指示方向．沿箭头方向移动对应于右乘生成元a．所以，以标记a^2的顶点作起点，沿着指向I的箭头方向移动就等价于

$$a^2a = a^3 = I.$$

与箭头反方向移动对应于右乘a^{-1}（即右乘生成元a的逆元素）．例如，以标记a^2的顶点为起点，沿着与指向a^2的箭头方向相反移动就等价于

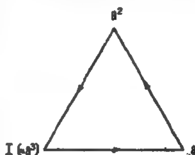


图 5.1

$$a^2a^{-1} = aaa^{-1} = a.$$

第六章　群　的　图　象

似乎在每一边画有箭头的多边形，能作为一个循环群的图示，即作为循环群的图象．让我们考察我们所知道的循环群的基本性质，并看看它们怎样与刚刚介绍的几何解释联系起来．

如果 a 是循环群的一个生成元，按定义我们知道，这个群的任何一个元素都能表成仅以 a 及 a^{-1} 作为因子的乘积． 反之，每一个仅以 a 及 a^{-1} 作为因子的乘积都是一个群元素．例如，考虑三个乘积：

$$a,\ aaa^{-1},\ a^{-1}aaa^{-1}a,$$

碰巧所有这些乘积都表示同一个群元素．

类似地，我们也将生成元和它们的逆元素的有限序列称为"字"．对于每一个含 a 及 a^{-1} 的字都对应于用 a 生成的循环群的一个元素．因为任何一个给定的群元素能用无限多种方法表示成一个字，所以用字作为群元素的解释不是唯一的．

若 x 是阶为 3 的循环群的某个元素，我们能将对应于 x 的任何一个字翻译成在假定的图象上的移动． 假设字 aaa^{-1} 表示 x，则我们可将这个字翻译成在图 6.1 中的图象上以如下方式作的移动：

1. 我们取标记 I 的顶点作起点．因为对应于 x 的字中的第一个因子是 a，所以我们从 I 出发沿与箭头相同的方向移动到线段的另一个端点(如图6.2所示)，这个端点是标记 a 的顶点，然后我们以它作为起点作进一步移动．

2. 因为在这个字中第二个因子是 a，所以当我们从所到

达的顶点开始移时仍沿与箭头相同的方向移动到线段的另一个端点(如图 6.3 所示),这个端点是标记 a^2 的顶点。以它作为起点再作进一步的移动.

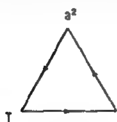


图 6.1



图 6.2

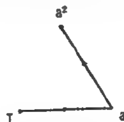


图 6.3

3. 因为第三个因子是 a^{-1}, a 的逆元素,所以我们从所到达的顶点开始时应沿与箭头相反的方向移动到线段的另一个端点,这个端点是标记 a 的顶点,它是任何进一步移动的起点.但这第三个因子已是这个特殊字的最后一个因子;因而已没有进一步的移动,所以对应于字 aaa^{-1} 的路的终端是标记 a 的顶点.

对应于 x 的字,可解释为在图象网络上沿道路移动的方向的集合. 每一个字,都对应于一个沿有向线段移动的特殊序列;反之,任何一条从 I 出发沿群的图象的有向线段移动的道路,都对应于一个特殊的字.

由于用有向线段的网络作为一个群的表示(其中的顶点对应于群元素,线段对应于右乘群的生成元或其逆元素)首先是十九世纪数学家凯莱(Cayley)引进的,所以这种网络或图象通常被称为凯莱图.

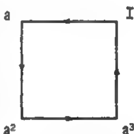


图 6.4

正方形在它所在平面内的诸旋转(第 6 页)构成一个阶为 4 的循环群. 这个群的图象如图 6.4

所示.

注

1) 循环群有多少个元素, 它的图象上就有多少个顶点.

2) 顶点 I 的位置是任意选择的.

3) 在每一个顶点有两条线段: 一条对应于右乘生成元 a, 箭头方向是远离该顶点; 另一条对应于右乘生成元 a 的逆元素 a^{-1}, 箭头方向是向着该顶点.

4) 图象网络采用什么特殊形状, 在这里并没有意义. 考虑的只是在诸顶点之间作内联而成一个图形. 若联接顶点的有向线段不用直线, 则图象的总的形状就不是正多边形. 只要不有损于数学意义, 你可以按你的美学观点随意选择你所喜爱的形状.

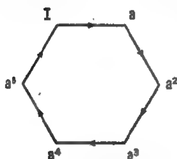


图 6.5

正 n 边形在所在平面内的诸旋转构成一个阶为 n 的循环群 C_n, 其图象是一个有向线段作成的 n 边形. 例如, 正六边形在所在平面内的诸旋转构成一个 6 阶循环群 C_6, 其元素是

$$a, a^2, a^3, a^4, a^5, a^6, (a^6 = I).$$

这个群的图象是一个有向线段作成的六边形, 如图 6.5 所示.

无限循环群

现在我们来构造无限循环群的图象. 循环群是用所有元素都能表示成某个生成元 a 的乘幂这个性质来定义的. 若存在一个正整数 n, 使得

$$a^n = I,$$

则说用 a 生成的群是有限的. 若不存在这样的正整数 n, 则 a 的每一个递增乘幂都表示群的一个新元素, 所以在这种情况下, 循环群是无限的. "无限加法群" (见 15 页) 就是这样的群.

为了构造无限循环群的图象，在心里记住几何图形是有帮助的．在有限循环群的情况下(即 n 为有限时)我们很容易得到对应的凯莱图．当 n 无限增大时，正 n 边形的边数无限增多，顶点到中心的距离无限增大．所以，不难想象，当 n 是 ∞ 时正 n 边形的周边已是一条无限长的直线，它的每一边是其上的一个单位线段．所以分成相等线段(每段长为 1)的直线(见图 6.6)就是无限循环群的图象．重合旋转就是在这条线上向右或向左移动一个或更多个单位．这个无限循环群的生成元是向右移动一个单位．



a^{-4} a^{-3} a^{-2} a^{-1} I a a^2 a^3 a^4

图 6.6

注

1) 根据我们的周期概念的自然推广，我们可用 C_∞ 来表示无限循环群．

2) 显然，任意一个顶点都可以取作 I．

3) 我们再一次看到，每一个顶点都有两条有向线段．沿有向线段作与箭头相同方向的移动对应于右乘生成元 a，沿有向线段作与箭头相反方向的移动对应于右乘 a 的逆元素 a^{-1}．

练习 8 确定加法在下列集合上是否是二元运算，并确定这些有二元运算的集合是否构成一个无限循环群：

(a) 4 的所有倍数的集合，也就是集合

$$\{\cdots, -8, -4, 0, 4, 8, \cdots\}.$$

(b) 整数 k 的所有倍数的集合．

(c) 集合 $\{\cdots, a-3, a-2, a-1, a, a+1, a+2, a+3, \cdots\}$，其中 a 不是整数．

(d) 集合 $\{\cdots, -3a, -2a, -a, 0, a, 2a, 3a, \cdots\}$，其中 a 不是整数．

有两个生成元的群

等边三角形的重合运动群的乘法表显示出，这个群有两个生成元：旋转 r 及翻转 f. 这个群的元素是(见 34 页)

$$I,\ r,\ r^2,$$
$$f,\ fr,\ fr^2,$$

容易看到，其中第一行的每一个元素是由它的左邻(或右邻)右乘 r (或 r^{-1})得到的;其中第二行的元素则分别是用它们上面的元素左乘 f 得到的. 这就提醒我们，对于这个群的图象要用两个以虚有向线段互连的三角形来表示(见图 6.7)，虚有向线段对应于生成元 f.

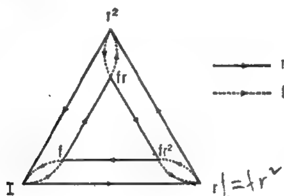


图 6.7

为了区别两个生成元 r 与 f, 在这个图象上我们用实有向线段表示乘 r, 用虚有向线段表示乘 f. 凯莱原来是用不同的颜色区别不同的生成元，他的图解表示法叫做群的着色表示法.

现在由于我们有两个生成元，所以在我们图象上的任何一条道路都能被仅由集合

$$r,\ f,\ r^{-1},\ f^{-1}$$

中的符号组成的序列所刻划. 序列

$$rfr^{-1}f^{-1} \text{ 和 } rf^{-1}rf^{-1}r$$

就是这种序列的两个例子，这种序列(如前所述)叫做字．当然，含有生成元或其逆元素的每一个字是群的一个元素，更严格地说是，每一个这样的字表示一个群元素．

读者应该自己验证，用这个群的乘法表（第 35 页）给出的任意两个元素的乘积，与由图 6.7 中的图象得到的乘积正好是一致的．例如，为了验证

$$rf = fr^2,$$

首先由起点 I 移动 r-线段，然后再移动 f-线段，到达标记 fr^2 的顶点（见图 6.8）．在图 6.9 中指出，路

$$frrf = r.$$



图 6.8

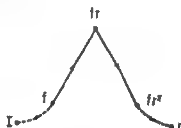


图 6.9

群的图象的基本性质

我们上面给出的那些不同群的图象的例子，却有某些共同的基本性质．

(1) 群元素 ⟷ 图象顶点．

即：群元素与图象顶点一一对应．这也就是说，群的图象上的每一个顶点恰好对应于一个群元素，且反之亦然．

(2) 生成元 ⟷ 相同"颜色"的边．

图象网络的每一边都是有向线段，相同"颜色"的有向线段对应于群的相同的生成元。由起点顺箭头方向沿线段运动，对应于右乘生成元 a；反箭头方向沿线段运动，对应于右乘生成元的逆元素 a^{-1}。若图 6.10 中的图象顶点 A，B 及 C 分别表

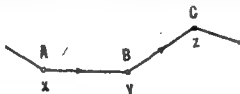


图 6.10

示群元素 x，y 及 z，则由 B 到 C 的运动就对应于 a 乘 y，所以

$$ya = z;$$

而由 B 到 A 的运动就对应于 a^{-1} 乘 y，所以

$$ya^{-1} = x.$$

(3) 字⟷道路.

表示群元素的每一个字可解释为一条道路（即图象的有向线段的一个特殊序列），且反之亦然。对于对应于一个字的道路，在一个顶点沿道路所作的下一个运动都被字的下一因子所规定。因为每一个因子或者是生成元或者是生成元的逆元素，所以图象的每一顶点是两条相同"颜色"的有向线段的端点：一条的箭头方向向着这个顶点，而另一条的箭头方向背离这个顶点。如果这个群有两个生成元 a 和 b，则在每一个顶点有四条边，这是因为从每一个顶点，对应于四个因子

$$a,\ a^{-1},\ b,\ b^{-1}$$

有四个可能的运动。一般地说，对于每一个生成元，在每一个

顶点有一条进入边和一条走出边.

(4) 元素的乘法⟷道路的相继.

两个群元素的乘法,对应于图象上的、用两个相继的道路合成的道路上的移动. 群元素 r 和 s 的乘积

$$rs = t$$

对应的道路可作如下的解释: 将 r 和 s 作为字中符号 (即生成元或其逆元素)来写. 用对应于 I 的顶点作起点,与其相接的道路是表示 r 的字所规定的道路. 这条道路的终点对应于 r. 然后再用 r-顶点作起点,与其相接的道路是表示 s 的字所规定的道路,(不管 r 和 s 表示什么特殊的字) 这条道路的终点对应于 $t = rs$.

(5) 表示 I 的字⟷闭道路.

任意一个表示 I 的字都对应于图象上的一条闭道路. 假设W是表示 I 的一个字. 例如,在等边三角形的重合运动群中,W可以是 $frfr$. 若对应于 I 的顶点被取作起点, 则被字W所规定的路将以 I-顶点为终点. 我们把起点与终点重合的道路称为闭道路. 若 t 不同于 I, 且取对应于 t 的顶点作起点,则被字W所规定的路将以 t-顶点为终点,这是因为 $tW = t$. 所以, 若W是表示 I 的字,则无论取什么顶点作起点,W所规定的道路都是闭道路. 具有这个性质的图象叫做是齐次的.

由群的图象的"齐次性"推得, 图象上的任意选择的一个顶点都可标记为 I (见练习 9, 第 56 页). 由 57 页的练习 11 看到, 有这样的例子, 其边是有向线段的图形不是齐次的, 这样的图形不是一个群的图象. 这类图形是有"缺陷"的, 练习

11 中的图形就有一条有向边重合为一个端点.

(6) $rx=s$ 的可解性 ⟷ 图象网络是连通的.

群的图象是连通的网络是指，从图象上的任一顶点到其他每一个顶点都有道路相连. 若 r 和 s 是群的任意两个元素，则有一个元素 $x=r^{-1}s$，使得 $rx=s$（第 36 页）. 显然，如果 W 是表示 $x=r^{-1}s$ 的任意一个字，则 $rW=s$；所以如果对应于 r 的顶点取作起点，则 W 所规定的道路是由 r-顶点到 s-顶点的道路.

我们将前面讨论中阐述的对应关系总结如下：

群	图象
元素	顶点
生成元	相同"颜色"的有向边
字	道路
元素的乘法	道路的相继
表示 I 的字	闭道路
方程 $rx=s$ 的可解性	网络是连通的

由于我们能够选择凯莱图的任意顶点与 I 对应，所以同样的群的图象表示似乎不需要标记顶点. 例如，在图 6.11 中的两个未标记顶点的凯莱图的每一个，都充分刻划了一个 4 阶循环群. 但是我们不应当走到试图消去边的有向记号. 考虑图 6.12 中的两个图象，它们的不同仅在于内三角形的边的箭头方向，但是它们所表示的群有本质差别，这是因为其中只有一个是交换群（见 57 页的练习 10）. 今后，如果需要澄清，就要标记群图象的顶点.

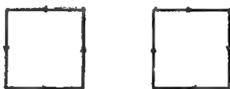


图 6.11



图 6.12

关于表示 I 的字的注 一字表示 I，当且仅当(群的图象网络上的)对应的道路是闭的(回想，当起点与终点重合时道路是闭的)．我们能区分闭道路的有本质差别的两种类型．图 6.13 是正三角形的运动群的图象(50 页)上的两条道路

$$I\to P\to Q\to I \text{ 及 } I\to R\to S\to T\to S\to R\to I$$

的图示，这两条道路都是闭的，但是不管是用拓扑学的观点还是用群性质的观点看，它们的本质都是不同的．拓扑学是几何



图 6.13

学的一个分支，它考虑的是几何对象的连接方式，而全然不考虑线的长度这样的性质. 如果几何图形的变形不破坏图形的任何线或接合处，则这种变换叫连续变换. 拓扑学仅仅考察几何图形在连续变换下保持不变的性质. 从拓扑学的观点看，对应于字 $W_1 = r^3$ 的道路与对应于字 $W_2 = fr^{-1}r^{-1}rrf^{-1}$ 的道路有本质区别：对应于 W_1 的闭路在每一个线段上只经过一次，从不经过两次，而对应于 W_2 的闭道路在每一个线段上都来回两次(读者应将道路 W_2 的特点与 38 页讨论过的群乘积的逆元素作一个比较).

群的公理是构成所有群的性质的基础. 从群的公理的观点也可以看出 W_1 与 W_2 之间的基本差别. $W_2 = fr^{-1}r^{-1}rrf^{-1}$ 在任何有二个元素(我们指定它们为 r 和 f)的群中都表示 I，但 $W_1 = r^3$ 仅在使 $r^3 = I$ 成立的那些特殊群中才表示 I.

为了看出 $W_2 = I$ 在任意群中都成立，我们只需写

$$\begin{aligned} W_2 &= fr^{-1}r^{-1}rrf^{-1} = fr^{-1}(r^{-1}r)rf^{-1} \\ &= fr^{-1}(I)rf^{-1} = fr^{-1}rf^{-1} = f(r^{-1}r)f^{-1} \\ &= f(I)f^{-1} = ff^{-1} = I. \end{aligned}$$

应用群的公理我们逐次消去了所有表示生成元及其逆元素的符号，因而将字 W_2 化简成 I. 我们称 W_2 为空字，因为应用群的公理它能表示成除 I 外不含其他任何群元素. 我们断定：

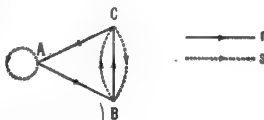
(1) 在图象网络的每一线段上都往返两次而返回自身的闭道路，对应于空字.

(2) 所有其他的闭道路对应于生成元之间的一个特殊关系，但这并不是对所有的群都是真的.

练习 9 在等边三角形的重合运动群的图象(图 6.7) 中，设取内三角形的原来标记 fr 的顶点作为 I，画出这个群的有对应标记的凯莱图.

练习 10 首先画出等边三角形的重合运动群的凯莱图，然后修改它：只改变内三角形的箭头方向．标记改变后的内三角形的顶点，然后作六个元素的乘法表，用修改后的图象来确定新的乘积．这个集合是一个群吗？

练习 11 下面是一个用两种类型（或两种“色”）的有向边 r 和 s 构成的图象．这个图象是连通的，并且在 A、B、C 三个顶点中的每一个都有四个（对应于字的四个可能因子 r，r^{-1}，s，s^{-1} 的）可能运动，但是可以证明，这个图象不可能是一个群的图象，这是因为，用 r 和 s 及它们的逆元素构成的字，在一个顶点对应于闭道路，在其他顶点却不是（例如，试试字 sr^3s 及 rsr）．



变现群的图象

已经看到，群的凯莱图能用任何方法变形，只要我们不破坏顶点之间的任何联接．例如，图 6.14 是等边三角形的重合运动群的凯莱图（见 50 页的图 6.7）的变形．这个群的这个凯莱图也可以变成三维网络，如图 6.15 所示．

这种三维图象有力地暗示了群的实际上的物理运动．下面的三角形 ABC 可以用来表示没有翻转的三角形的位置，其箭头表示三角形在所在平面中的运动，上面的三角形 DEF 则刻划翻转后的三角形位置，其箭头表示翻转后再旋转的三角形的位置．在每一个顶点处的构成闭圈的一对线段表示来

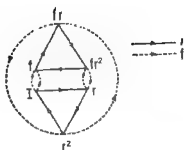


图 6.14

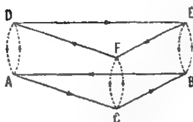


图 6.15

回翻转.

这里是首先画出凯莱图，然后修改成符合物理作用的图示. 有时我们颠倒这个过程，首先画群的实际运动的图形表示，然后抽象成那个群的凯莱图.

二面体群

考虑导致一个正方形重合于它自身的运动的集合——正方形的重合运动. 等边三角形的情况提示我们，这些运动的生成元是 r（正方形在所在平面旋转 90° 的运动）和 f（正方形绕对角线转 180° 的翻转）. 这些运动指出，三维表示如图 6.16 所示. 这个图象是以 r 和 f 为生成元的，满足

$$r^4 = I \text{ 及 } f^2 = I$$

的 8 阶群的凯莱图. 若把它变成二维网络，则如图 6.17 所示.

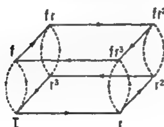


图 6.16

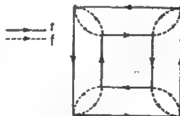


图 6.17

任意正多边形的重合运动的情况，与等边三角形的情况的类似性是非常显然的，因而可直接推广到任意正多边形的重合运动群.

正多边形的重合运动群叫做二面体群. “二面体”表示“两个平面”，因而，我们可以看到，一个二面体群的凯莱图的三维型式表示成两个平面多边形，它们的顶点被生成元“翻转”线段所联接. 今后我们将用D作为二面体群的一般符号. 我们也将用下标表示这个群的多边形的顶点的个数. 因此，等边三角形的六阶二面体群将用D_3表示；正方形的八阶二面体群将用D_4表示. 一般地，正n边形的二面体群，我们将用D_n表示. 显然，D_n是一个$2n$阶群.

有一个周期为2的生成元的群的图象的画法，有一个简化方法. 因为二面体群的“翻转”元素f是周期为2的，所以我们将用二面体群的图象来阐明这种简化方法，但它也适用于有周期为2的生成元的任何群的图象.

所有含有周期为2的生成元(如f)的图象，在每一个顶点都有一对f-线段的“闭圈”. 我们仍用每一对这样的线段表示f和它的逆元素f^{-1}. 我们可以省略这种（从一条线段上出去又回来的）所用的箭头，而仅用一条没有箭头的线段来表示周期为2的生成元. 因为对于周期为2的生成元有$f=f^{-1}$，所以沿每一个方向移动f-线段就表示右乘f或f^{-1}. 用这种



图 6.18

简化方法来画二面群 D_3 和 D_4 的图象，就如图 6.18 所示. 注意，生成元 r（它的周期大于 2）是用有箭头的线段表示的，只是对应于（周期为 2 的）f 的线段才没有箭头.

第七章　按生成元和关系定义群

我们已经看到，一个特殊的群可用下面这些方法定义：

(i) 有二元运算且满足三个群公理的（一些元素的）集合．这是基本定义形式，所有其他可能的定义方式都是由它推导来的．

(ii) 具有在第四章中所讨论过的一些性质的、我们叫做群的乘法表的(一些符号的)方阵．这种方阵以规定群元素的所有乘积的方式来定义一个群．

(iii) 满足我们对群的图象所规定的一些基本性质的(一些有向线段的)网络．这种网络用规定它里面的结构(即群元素的任何一个乘积对应于这个图象网络上的什么相继的路)的办法来定义一个群．

在这一章，我们将专门指出，还有其他定义群的方法——用生成元和它们的关系来定义群的方法．关于生成元，我们已有某些经验．

循环群 C_3

我们将由检验（用 C_3 表示的）3 阶循环群的简单情况开始．这是等边三角形在其所在平面内的旋转群（16 页）．这个群 C_3，(作为一个循环群）能用它的一个元素（如 r）生成，而且它的 3 个元素能表示成

$$r, r^2, r^3(=I).$$

现在我们来考虑这相反的情况：

(1) G 是用一个元素 r 生成的，

(2) $r^3 = I$.

这些条件能完全确定G的结构吗？特别是群G必须是一个3阶循环群吗？回答是"不能"。这是因为我们仅仅考察关系$r^3 = I$是不够的，如果还满足$r = I$，则就看出这个群G可以仅由一个元素I组成，所以是1阶的。因此，如果我们想完全确定G，我们就必须修改我们对群G的刻划。显然，若命题(2)修改成

(2′) G的定义关系的集合仅由一个关系$r^3 = I$构成，

则(1)和(2′)就能完全确定作为一个3阶循环群的G。为了阐明这个命题，我们必须给出"关系"的精确含义，然后再给出一个群的定义关系的含义。这以后我们才能够决定C_3的"关系"$r^3 = I$是否是C_3的一个定义关系。

一个关系涉及一个如下的等式：

$$W = I,$$

其中W是群的一个字(见46页)。字W有两种不同的类型，对于它们我们都可以有$W = I$。首先在C_3中有这样的字rrr或r^3，对于它，命题

$$r^3 = I$$

断言，字表示一个与I相同的群元素。这个等式不是群的公理的一个推论，因而对于所有的群一般是不真的。例如，在生成元为r的循环群C_2中$r^3 = I$就不真。相反，考虑命题

$$rr^{-1} = I;$$

这个等式是群的公理(逆元素公理)的直接推论，因此对每一个群的每一元素r都成立。注意，rr^{-1}是空字；对所有的生成元，我们都可以应用群的公理，并可以用I取代互为逆元素的元素对(见56页)。但r^3不是空字，因而仅仅在特殊的群中$r^3 = I$才是真的。让我们约定，在我们的关系的定义中，对于$W = I$，我们将排除W是空字的平凡情况。我们应回忆起，

命题 $r^3 = I$ 和 $rr^{-1} = I$ 都对应于 C_3 的闭道路，后者对应于返回自身的平凡的闭道路，而前者则对应于非平凡的闭道路(见 55 页).

我们将利用的**群关系**的定义：若 W 是群 G 的非空的字，且使

$$W = I,$$

则称这个等式是 G 的一个关系．因为字 W 是 G 的生成元的乘积，所以我们也称 $W = I$ 是 G 的一个生成元关系[1]．

为了引进 G 的**定义关系**的概念，我们考虑由 G 的所有非平凡关系组成的集合，即集合

$$\{R_k = I\},\ k = 1, 2, \cdots,$$

其中 R_k 不是空字．我们将用 A 标记关系 $R_k = I$ 的集合．

让我们来考虑关系集合 A 是空集合（没有任何元素的集合）的情形．难道有一种群它没有生成元关系吗？仅仅由一个元素 I 组成的平凡群可以作为没有生成元关系的群．然而我们也应考虑用指明有(例如)满足关系 $a = I$ 和 $b = I$ 的生成元 a 和 b 的方法来确定同一个群．在这种情况下，每一个字等于 I．让我们回避这种情况，而仅考虑至少有一个字不等于 I 的群．用元素 a 生成的无限循环群 C_∞ 就是这样一个群．我们已经看到(48 页)，若 C_∞ 的任何一个字是非空的，则它不等于 I，因为 $n \neq 0$ 时 $a^n \neq I$；这就是说，群 C_∞ 没有仅含有单个生成元 a 的关系．用一个元素生成的无限循环群 C_∞ 是一个没有关系的群．这样的群叫做**自由群**．

假设集合 A 至少包含一个关系 $R = I$，我们将指出，只要对关系 $R = I$ 应用群的公理，A 就包含无限多个关系．特

[1] 好象我们应考虑更一般的形式 $W_1 = W_2$ 作为群 G 的一个关系；但是用群公理能将其变形为 $W = W_1W_2^{-1} = I$，所以仅考虑形如 $W = I$ 的关系就够了．

别是，若 $R = I$，则

$$R^{-1} = I\ (\text{因为 } RR^{-1} = I),\quad R^2 = R \cdot I = I.$$

类似地，$R^{-2} = I$. 继续乘等于 I 的字，我们得到

$$R^n = I \text{ 及 } R^{-n} = I,\ (n = 1, 2, \cdots).$$

这个结果指出，由一个关系 $R = I$ 就可推出无限多个关系，因而 A 必须包含无限多个关系 $R_k = I$，其中 R_k 是非空字.

关系 $R^n = I$ 和 $R^{-n} = I$, $n = 1, 2, \cdots$, 不仅仅是由一个关系 $R = I$ 和群的公理推导出来的. 显然，若 W 是用群 G 的生成元作成的任何一个字，则

$$W^{-1}RW = W^{-1}IW = I \quad \text{且 } W^{-1}R^{-1}W = W^{-1}IW = I;$$

而且可以指出，由 $R = I$ 推出的所有关系的集合是由形如 $W^{-1}RW$ 和 $W^{-1}R^{-1}W$ 作因子的所有等于 I 的乘积构成的一个集合.

现在我们转向群 G 的所有非平凡关系的集合 A，而且如果可能我们将选择这样的子集 B，用 B 中的关系能推得 A 中的所有关系. 关系的这种集合 B 叫做群 G 的**定义关系集合**. 我们可以确信，如果 A 是非空的，则至少有一个定义关系集合，这是因为我们总可以取集合 A 自己作为 B. 更有兴趣的且更有用的情况是，B 是 A 的一个真子集(即 B 与 A 不完全一样).

在详细叙述特殊的群之前，我们先来阐明"由集合 B 的关系推得集合 A 的所有关系"的含义. 我们的意思是说，应用群的公理我们能从 B 的关系推得 A 的所有的关系；例如，在上面我们已经看到，由一个关系 $R = I$ 组成的集合怎样推导出无穷多个关系

$$R^n = I,\ R^{-n} = I,\ W^{-1}RW = I \text{ 及 } W^{-1}R^{-1}W = I.$$

现在我们来研究关系

$$r^3 = I$$

是否是生成元为 r 的 3 阶循环群 C_3 的定义关系．首先回忆：用 r 和 r^{-1} 排成的每一个字都可以写成 r 的幂次，所以，C_3 的所有关系的集合 A 为

$$A = \{r^{3k} = I\},\ k = \pm 1,\ \pm 2,\ \cdots.$$

注意，集 A 也可以写成如下的形式(见 22 页)：

$$A = \{r^n = I\},\ n \equiv 0 (\mathrm{mod}\ 3),\ n \neq 0.$$

C_3 的每一个非平凡关系都已包含在集合 A 中；这是因为，若 $r^{3k+1} = I$ 是 C_3 的一个关系，则将推得 $r = I$．但在群 C_3 中 $r \neq I$，因此 $r^{3k+1} \neq I$．类似地，由 $r^{3k+2} = I$ 可推得 $r^2 = I$，这个关系在 C_3 中也是不成立的．

我们认为，我们取一个关系

$$r^3 = I$$

就能组成 C_3 的定义关系集合 B．集合 A 的每一个关系都可由这个关系和群公理推得．例如

$$r^3 = I \text{ 推得 } r^{-3} = I,$$

因而

$$(r^3)^k = I,\ (r^{-3})^k = I,\ k = 1,\ 2,\ \cdots.$$

所以，$r^3 = I$ 推得

$$r^n = I,\ n \equiv 0 (\mathrm{mod}\ 3),\ n \neq 0,$$

而这些正好是 A 的所有的关系（从我们的关系集合中排除 $n = 0$ 的情况，是因为 r^0 是空字）．

对于 C_3，还有其他的定义关系集合，例如单个关系 $r^{-3} = I$，或两个关系 $r^6 = I$ 及 $r^{-9} = I$ 也可以取作集合 B．

下面的定理充分给出了定义关系概念的完整的潜在意义．这个定理断言，在任意生成元集合上的任意生成元关系的集合完全确定一个群．

定理 2 若我们给定一个关系 $R_n = I$ 的集合 B，其中每一个 R_k 是用一组生成元符号给出的非空的字，则存在一

个群 G, B 是它的生成元关系集合.

定理 2 的证明超出了本书的范围. 然而, 对于两个具体的定义关系集合,我们将详细说明这个定理.

我们需要用到等价字的概念. 考虑两个字

$$W_1 = rr^{-1}r \text{ 和 } W_2 = r^{-1}rr.$$

把它们看作是生成元和其逆元素的序列,这两个字是不同的,这是因为第一个(和第二个)符号是不同的. 但是把它们看作是群元素的表示时,则它们表示同一个群元素,这是因为

$$W_1 = rr^{-1}r = (rr^{-1})r = Ir = r$$

及

$$W_2 = r^{-1}rr = (r^{-1}r)r = Ir = r.$$

如果两个字 W_1 与 W_2 表示同一个群元素,则说它们是等价的.

注意, 在所出现这些序列中,我们删去 $rr^{-1}=I$ 和 $r^{-1}r=I$ 而将 W_1 和 W_2 "变换"为 r, 现在我们在循环群 C_3 中考虑字

$$W_3 = r^{-1}r^{-1} \text{ 和 } W_4 = rrrr.$$

我们已经看到,这个群被关系 $r^3 = I$ (由它可推得关系 $r^{-3} = I$) 所确定. 现在我们用插入及删去等于 I 的字的办法来"变换"字 W_3 及 W_4:

$$\begin{aligned} W_3 &= r^{-1}r^{-1} = (rr^{-1})r^{-1}r^{-1} && \text{(插入)} \\ &= r(r^{-1}r^{-1}r^{-1}) = rr^{-3} = rI = r && \text{(删去)} \end{aligned}$$

及

$$W_4 = rrrr = r(rrr) = r(r^3) = rI = r. \qquad \text{(删去)}$$

不同的字 W_3 与 W_4 在循环群 C_3 中却表示同一个群元素;我们说 W_3 与 W_4 在 C_3 中是等价字.

等价概念可以推广到任意符号集合上的任意两个字 W_1 与 W_2: 如果删去或插入等于 I 的字可将 W_1 变换成 W_2, 则说 W_1 等价于 W_2. 因为删去和插入等于 I 的字的运算是可逆的, 所以也可将字 W_1 变成字 W_2 的步骤"颠倒"过来而将字 W_2 变成字 W_1. 这说明如下的命题是正确的: 如果 W_1 等价于 W_2,

则 W_2 等价于 W_1. 可以证明，如果 W_1, W_2 和 W_3 是这样的字，W_1 等价于 W_2，W_2 等价于 W_3，则 W_1 等价于 W_3. 我们所期望和要求的这个性质叫做关系的"等价性"❶.

我们将利用等价性概念把字的集合划分成等价字的类. 设 F 是给定的符号集合上的所有字的集合；也就是说，F 是所有用表示生成元和它的逆元素的符号排成的有限序列. F 的所有的字的分类法如下：若 W_1 和 W_2 是 F 的等价字，则 W_1 和 W_2 归入同一类；若 W_1 与 W_2 是 F 中的不等价的字，则它们不能归入同一类. 换句话说，W_1 和 W_2 归入同一类，当且仅当它们是等价的.（一般问题怎样解决，对任意给定的群，两个字实际上是否等价，是非常困难的. 这个问题，通常叫字问题，只有很少的群被解决.）F 怎样被划分为等价字的类，下面在我们讨论被关系 $r^3=I$ 确定的群时，将给出一个例子. 那时 F 将被划分为等价字的类，等价的字将用同一个群元素表示. 我们可用某一类中的任意一个字作为这个类的代表元❷.

现在我们来详细说明定理 2（65 页），下面我们将介绍一个基本方法的要点. 介绍是抽象的并采用一般术语，后面将用详细说明的例子来巩固它.

(1) 我们给定一个生成元符号的集合和关系 $R_k=I$ 的集合 B（这里每一个 R_k 都是用给定符号拼成的非空的字）.

(2) F 是所有（用给定符号拼成的）字的集合.

(3) 将 F 的所有使得 $W=I$ 的字 W 作成子集 K，这里的 $W=I$ 是由给定的关系 $R_k=I$ 的集合推出来的.

(4) 将 F 划分成等价字的类（等价的字即是可以用删去

---

❶ "等价性"的更正式的提法可参阅本丛书的第 9 本：C. D. Olds 的 "Continued Fractions"（连分数）的 127 页.

❷ 在旋转群（第 17 页）和"模 2 相等"的讨论（第 21 页）中，我们实际上已经利用过类的代表元.

或插入等于 I 的字的方法彼此互变的字).

(5) 选择代表元字的集合 G (代表元字是从每一个等价类中选来的一个字). 任意这样的集合 G 是一个群 (对这个群,给定关系 $R_k = I$ 是定义关系).

关于 K 的构造的注 我们要求, K 是形如 $T^{-1}RT$ 或 $T^{-1}R^{-1}T$ 的字的所有乘积(即有限序列)的集合, 这里 $R = I$ 是给定集合 B 中的一个关系, 而 T 是 F 的任意的字. 若 $R = I$, 则显然所叙述的任意一个字都等于 I, 这是因为 $T^{-1}IT = I$. 反之,若 V 是 F 的一个字, 且由我们的关系能推得 $V = I$, 则 V 是形如 $T^{-1}RT$ 的因子的乘积.

用定义关系确定 C_3

(1) 我们应用前面的方法来"发现"有一个生成元 r 的、由定义关系 $r^3 = I$ 确定的群 G (无疑我们"希望"群 G 结果是一个 3 阶循环群).

(2) 我们的字是用符号 r 和 r^{-1} 组成的有限乘积, 所有这样的字就组成我们的集合 F. 显然, F 的任意一个字 T 都能变成 r 的乘幂,即 T 可变为 r^n, $n = 0, \pm 1, \pm 2, \cdots$.

(3) 在当前的情况下, 形如 $T^{-1}RT$ 或 $T^{-1}R^{-1}T$ 的字也就是形如

$$(r^n)^{-1}(r^3)(r^n) \text{ 或 } (r^n)^{-1}(r^{-3})(r^n)$$

的字. 为了作成集合 F, 我们来寻找所有形如

$$(r^n)^{-1}(r^3)(r^n) \text{ 或} (r^n)^{-1}(r^{-3})(r^n)$$

的字"生成"的字. 但是, 如果我们从这些字中消去所有相邻的互逆对时,它们就变成

$$r^3 \text{ 和 } r^{-3}.$$

所以集合 K 包含有 r^3 和 r^{-3} 的乘幂:

$$K=\{r^n\},\ n\ 是\ 3\ 的倍数,$$

即

$$K=\{r^n\},\ n\equiv 0(\bmod 3).$$

K 的所有这些等于 I 的字都可由关系 $r^3=I$ 推得.

(4) 用删去或插入所有 $n\equiv 0(\bmod 3)$ 的字的方法来变换 F 的字 r^n. 我们看到,F 的字被划分为如下三个类:

A: $n\equiv 0(\bmod 3)$ 的字 r^n, 例如 $n=6$ 的字 r^6;

B: $n\equiv 1(\bmod 3)$ 的字 r^n, 例如 $n=4$ 的字 r^4;

C: $n\equiv 2(\bmod 3)$ 的字 r^n, 例如 $n=-1$ 的字 r^{-1}.

(5) 选出每一类的代表元:

$$A\ 选\ I(n=0),\ B\ 选\ r,\ C\ 选\ r^2.$$

(这种选法是方便的,但选法可以任意. 我们也可这样选代表元: A 选 r^3, B 选 r^{-2}, C 选 r^5.) 这三个代表元 I, r, r^2 作成一个群,即生成元为 r 的 3 阶循环群. (我们应回忆起类的等价字的含义. 例如,字 $(r^2)(r^2)=r^4$ 与字 r 在同一个类,因此我们能说群元素 $(r^2)^2$ 与群元素 r 相同.)

我们看到,被关系 $r^3=I$ 定义的群 G 正是我们所"期望"的 3 阶循环群.

D_3 的定义关系集合

我们将应用同样的基本方法来发现 D_3 是怎样被定义关系所确定的. 我们的首要任务是寻找关系集合(我们可以希望它结果是定义关系集合). 一个线索是在群的图象中寻找,因此我们来重新检查 D_3 的图象(见图 7.1).

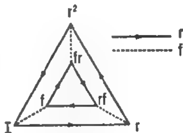
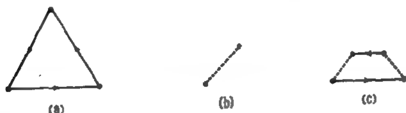


图 7.1

我们从用 r 和 f 组成的字中引出等于 I 的字，从而求得关系的集合. 我们回忆起，一个群中的每一个关系都联带它图象上的一个（非平凡）闭道路. D_3 的图象上的非平凡闭道路如图 7.2 所示. 道路 (a) 对应于关系 $r^3 = I$，道路 (b) 对



(a)　　(b)　　(c)

图 7.2

应于 $f^2 = I$，路 C 对应于 $rfrf = I$. 注意，这样的闭道路起自图象的每一个顶点，这由群的图象的齐次性（见 53 页）是可料到的.

我们要求

$$r^3 = I,\ f^2 = I,\ rfrf = I$$

是 D_3 的定义关系.

用关系集合定义 D_3 仍用我们的基本方法.

(1) 我们的生成元集合是 $\{r, f\}$，我们的定义关系是

$$r^3 = I,\ f^2 = I,\ rfrf = I.$$

(2) F 是所有用 r, f, r^{-1}, f^{-1} 组成的字的集合. 与上述的例子相反，没有简单的方案来记述所有这些字.

(3) 子集 K 包含所有由给定关系推得的、等于 I 的字. 我们来注意 K 的一个特殊的、后面要用到的字. 考虑用形如 $T^{-1}RT$ 或 $T^{-1}R^{-1}T$ 作为因子的字 V：

$$\begin{aligned} V &= f^{-2}(f^2)f^2 \cdot f^{-1}(rfrf)f \cdot r^{-3}(r^{-3})r^3 \\ &= f^2 \cdot f^{-1}(rfrf)f \cdot r^{-3} = f(rfr)(f^2) \cdot r^{-3} \\ &= frfr^{-2}. \end{aligned}$$

因为 V 在 K 中，所以

$$V = frfr^{-2} = I \text{ 即 } fr = r^2f.$$

(4), (5) 现在我们用删去或插入等于 I 的字的方法来变换 F 的字，并将 F 划分成等价字的类. 我们断言，有以

$$I, r, f, r^2, rf, fr$$

为代表字的 6 个等价字的类.

为了证明这个断言，我们将首先指出，不能有多于 6 个等价字的类，也就是说，F 中的任意的字都能变成这 6 个字中的一个；然后指出这 6 个字中没有两个是等价的. 为此，我们将利用 K 的每一个字都等于 I 的事实，并将利用 K 的那个特殊的字 V.

在 (3) 中我们已看到，因为 V 在 K 中，所以由

$$V = f^2 \cdot f^{-1}(rfrf)f \cdot r^{-3}$$

推得●

$$fr = r^2f.$$

利用该结果我们可以断定，F 中的每一个字都等于形如 $r^a f^b$ 的字，其中 a 和 b 是非负整数. 这是因为，对 F 中的给定的任意字，我们可以利用等式 $fr = r^2f$ 来"交换" f 与 r，而且是用 r^2 代替 r；用这种方法，我们可以把所有符号 f "移"到右边，把所有符号 r "移"到左边，而得到最后的字(在这种字中已用所有的符号 r 代替了所有的符号 f). 进一步，因为由关系 $r^3 = I$ 及 $f^2 = I$ 推得 $r^{-1} = r^2$ 及 $f^{-1} = f$，所以在变换出来的字中的所有 r 和 f 的幂次都可以假定是非负数. 因此正如我们所断言的 F 的每一个字都等价于形如 $r^a f^b$ 的字. 作为这个方法的一个具体说明，考虑如下的

● $fr = r^2f = r^{-1}f$ 是下列更一般结果的一个特殊情况：由两个关系 $f^2 = I$ 和 $rfrf = I$ 推得 $fr^n = r^{-n}f$ (对所有整数 n)；而且由单个关系 $rfrf = I$ 推得 $f^a r^b = r^x f^y$，其中 $x = (-1)^a b$，$y = (-1)^b a$.

$$r^2fr^2fr = r^2(fr)rfr = r^2(r^2f)rfr = r^4frfr$$
$$= r(fr)fr = r(r^2f)fr = r^3f^2r = r.$$

由 $r^3 = I$ 及 $f^2 = I$ 可进一步推得，每一个字 r^af^b 等价于形如 $r^{a'}f^{b'}$ 的字，其中 $a' = 0, 1$ 或 2，$b' = 0$ 或 1；也就是说，F 的每一个字等价于字

$$I,\ r,\ f,\ r^2,\ rf,\ r^2f(= fr)$$

中的一个.

至此，我们的论证证明，F 的等价字至多有 6 个. 然而，在以 I, r, f, r^2, rf 及 fr 作代表元的 6 个类中，或许有某些有共同的元素；也就是，我们提到的代表元的某些或许是可相互变换的字.留待证明的是，没有这种情况—— 6 个字中没有两个是等价的. 这种证明的实质部分是指出 $r \neq I$ 及 $f \neq I$. 虽然在我们的定义关系集合中并没有 $r = I$ 及 $f = I$，我们也不能假定这些量就不是我们提到的关系(能推得)的结果[1].

我们首先证明 $f \neq I$. 若 $f = I$ 是给定关系的一个结果，则 f 是 K 的一个字. 因此在 K 中存在一个用形如 $T^{-1}RT$ 或 $T^{-1}R^{-1}T$ 的因子作的字，它可以转变为字 f. 我们需要证明的是，无论我们怎样应用群的公理及给定的关系，都不能将 f 写成这些因子的乘积. 我们的方法的实质是，在 K 的任意字中检验 f 的指数和.我们将求可能因子 $T^{-1}RT$ 加到和上去的贡献. R 是字 $r^3, f^2, rfrf$（或它们的逆元素）中的一个，在这些字中 f 的指数和是 0, 2, 2（对于它们的逆元素则为 0, －2, －2).因为 T 是 F 的任意字，所以在 T 中 f 的指数和是任意的（例如 t）值. 因而 f 在 T^{-1} 中的指数和为 $-t$（应记住的是，如果 $T = r^2fr^{-3}f^3$，则 $T^{-1} = f^{-3}r^3f^{-1}r^{-2}$，见 38 页的关于乘积的逆元素的讨论). 在任何因子中 T^{-1} 和 T 的净贡献为 0.

---

[1] 例如，由两个关系 $xyz^2 = I$ 及 $z^2 = I$ 就推得 $y = I$.

因此，在任何因子 $T^{-1}RT$ 中 f 的指数和是 0，2 或 -2 中的一个．所以在 K 的任意字中 f 的指数和应为偶数．因为 f 有指数和 1（不是偶数），所以推得 f 不能在 K 中．

如果我们试图应用"指数和"的方法去证明 $r \neq I$，那就会发现根本行不通．这是因为，在形如 $T^{-1}RT$ 的字中 r 的指数和可以是 0，2 或 3 中的一个，所以在 K 的字中偶数和及奇数和都能出现．我们将应用前面的 D_3（全等三角形的重合运动群）的存在性知识来证明 $r \neq I$．假设 $r = I$ 真是关系

$$r^3 = I,\ f^2 = I,\ rfrf = I$$

推得的一个结果，则这个结果在这些关系为真的任何群中都成立．我们知道在特殊群 D_3 中这些关系是真的，但在 D_3 中却没有 $r = I$．因此 $r = I$ 不是给定关系的一个结果．

$r = f$ 能作为给定关系的一个结果吗？若 $r = f$，则 $r^2 = fr = r^2f$，它推得 $f = I$．但 $f \neq I$，所以 $r \neq f$．

我们已证明 I，r，f 是不等价的．留给读者作为练习的是，证明我们的 6 个代表元的集合中剩下的字互相不同，而且与 I，r，f 也不相同．例如，能有 $r = r^2$ 吗？显然由它推得 $r = I$，如此等等．

练习 12　群 D_3 的定义关系集合是

$$A:\ r^3 = I,\ f^2 = I,\ rfrf = I,$$

证明 D_3 也可被关系集合

$$B:\ f^2 = I,\ frfr^{-2} = I$$

定义．［提示：已知集合 A 能推得集合 B（见 71 页），因此，如能证明集合 B 推得集合 A 就证明这两个关系集合是等价的；每一个集合都定义同一个群．］

现在我们希望读者更直接地应用基本方法做如下的练习 13 至练习 17．如有困难，等到对本书有进一步了解之后再

做也可.

练习 13 假设G是一个群,其生成元是x和y,它们满足关系

$$x^2 = I, \quad xyx^{-1} = y^n \ (\text{其中}\ n > 1).$$

证明

$$y^{n^2-1} = I.$$

练习 14 (a) 设u和v是群H的元素,并假设

$$u^3 = I, \quad uvu^{-1} = v^4,$$

证明v是一个有限周期的元素.

(b) 假设群H有元素u及v,使得

$$u^m = I, \quad uvu^{-1} = v^k,$$

其中m和k是整数,$k > 1$, $m \neq 0$,证明v是一个有限周期的元素.

练习 15 证明存在一个16阶的群,它的两个生成元x及y满足关系

$$x^2 = I, \quad xyx^{-1} = y^3.$$

希望在证明中将包含作这个群的图象.

练习 16 证明,若G是两个生成元s和t生成的、满足关系

$$s^n = I, \quad sts^{-1} = t^k$$

(其中n和k是整数,$n \neq 0$, $k > 1$)的任意群,则G是有限阶的. 并证明G的不同元素不能多于$(k^n - 1)n$个. [提示:利用71页证明中应用的技巧,即:由等式$fr = r^2f$可推得,D_3所有的字都能变成形如r^af^b的字.]

练习 17 在前一练习中设 $n=3$, $k=2$. 证明却存在一个 21 阶的群,它有两个生成元 s 和 t, 满足

$$s^3=I,\ sts^{-1}=t^2,$$

做这个练习时画出这个群的图象.

二面体群 D_n 的生成元及关系

我们曾对一个二面体群(即 D_3)的定义关系作过详细的讨论. 用同样的基本方法可证明如下的一般命题: 一般二面体群 D_n 完全被条件

(1) D_n 是由两个记为 r 和 f 的元素生成的,

(2) 这两个生成元满足三个定义关系:

$$r^n=I,\ f^2=I,\ (rf)^2=I$$

(用关系集合作为定义关系的含义, 在 64 页的讨论中已经明确过).

二面体群 D_n 当 n 较小时的特殊情况,特别有趣.当 $n=1$ 时,二面体群的定义关系变为

$$r=I,\ f^2=I,\ (rf)^2=I.$$

因为 $r=I$ 推得 $(rf)^2=f^2=I$,所以只留下 $f^2=I$ 及 $r=I$ 作为定义关系. 但这些关系定义二阶循环群, 所以, $D_1=C_2$. 可看出这一点的另一种方法, 是将 D_1 作为只有一边的"多边形"(即线段)的重合运动群考虑. 线段的两个重合位置是

1 ●——● 2　　2 ●——● 1

用(59 页的)简化方式画的 D_1 的图象为

I ●- - - - - - - - - - -● f

当 $n=2$ 时, D_2 的定义关系是

$$r^2=I,\ f^2=I,\ (rf)^2=I,$$

即

$$r^2=f^2=(rf)^2=I.$$

我们将按"二边形"的解释来构造 D_2 的图象，"二边形"是二边平面图形，其边是弧． 图 7.3 是这个二边形的重合运动的一个图示，这里 r 是一个旋转，f 是一个翻转．如果我们考虑前面（51 页）建立的群的图象性质，则我们看到，我们的二边形的重合运动的表示却是 D_2 的凯莱图．

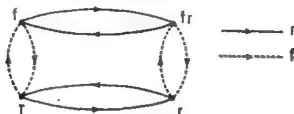


图 7.3

利用周期为 2 的生成元的简化表示（且注意到 r 和 f 都是周期为 2 的）时，我们能将 D_2 的图象简化为图 7.4. 注意，与 I 成对角的顶点曾标记为 fr，但图象显然表示，对应于字 fr 的道路与对应于字 rf 的道路把 I 引向同一顶点，所以有 $rf=fr$，因而 D_2 是一个交换群．



图 7.4

阶为 4 的群 D_2 常简称为四群，也可按关系的指数简称为二次群．当研究正四面体的重合运动时，我们将再次遇到这个群．

可交换的二面体群

D_1 和 D_2 都是可交换的，但一看 D_3 和 D_4 的图象（59 页）

即知它们是不可交换的．我们能对二面体群 D_n 的可交换性给出一个一般命题吗？可以，我们将指出，D_1 和 D_2 是仅有的可交换二面体群．

定理 3 仅当 $n=1$ 及 $n=2$ 时，二面体群 D_n 的生成元 r 和 f 的定义关系

$$r^n=I,\ f^2=I,\ (rf)^2=I$$

才可推得

$$fr=rf;$$

反之，若 $n>2$，则二面体群 D_n 是不可交换的．

为了证明这个定理．我们首先观察，在任何可交换的二面体群中有

$$I=(rf)^2=(rf)(rf)=(rf)(fr)=rf^2r=r^2.$$

若 n 是偶数，由 $r^2=I$ 推得 $r^n=I$，所以原来的 D_n 的定义关系等价于 D_2 的定义关系

$$r^2=I,\ f^2=I,\ (rf)^2=I.$$

若 n 是奇数，例如 $n=2k+1$，则

$$r^2=I=r^n=r^{2k+1}=r^{2k}r=Ir=r,$$

所以 $r=I$，因而 D_n 的原来的定义关系等价于 D_1 的定义关系

$$r=I,\ f^2=I.$$

这就完成了我们的证明．

二面体群 D_∞

有无限阶二面体群 D_∞ 吗？我们将用展示它的图象的方法来证明其有．D_∞ 的图象是由 r-线段组成的并被 f-线段互连的两个 n 边形．如果我们回想起 C_∞ 与 C_n 的图象是怎样相关的(n 边形的边数由 n 增加到无限多，即由 C_n 变为 C_∞ 的

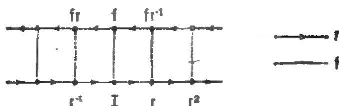


图 7.5

图象)，则当我们将(互连的)两个 n 边形用两条互连的平行直线代替(见图 7.5)时，似乎我们也能由 D_n 得到 D_∞ 的图象。这个直线段网络满足群的图象的所有性质。我们将用 D_∞ 表示与其对应的群。

现在让我们用生成元和定义关系的观点来检验 D_∞。我们看到，首先 D_n 的定义关系

$$r^n = I,\ f^2 = I,\ (rf)^2 = I$$

对 D_∞ 的图象并不有效。(类似地，在 C_∞ 的情况中，关系 $a^n = I$ 也不成立，因而应去掉，见 48 页。) 我们去掉关系 $r^n = I$ 而仅保留

$$f^2 = I,\ (rf)^2 = I$$

以定义 D_∞。关系 $f^2 = I$ 需要在 D_∞ 的图象的每一顶点画一对弧，在简化形式中则需要在每个顶点画一条 f-线段。关系 $(rf)^2 = I$ 对应于一个四边形，它的边是 r-线段与 f-线段相交替。在图 7.5 中正好都有这些性质。

直积

所有二面体群的凯莱图都给人一个"双重"循环群的直观印象。群 D_n 表示为 r-线段的(被 f-线段互连的)两个 n 边形。群 D_∞ 则表示为 r-线段的(被 f-线段互连的)两条平行直线。这使我们联想到，新的扩大的群有时可以用小的群"组合"而成。

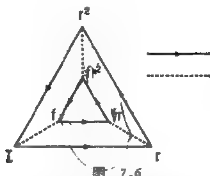


图 7.6

我们来考虑，在二面体群的图象中，只改变一个多边形的边上的箭头方向，并重新标记对应的顶点．图 7.6 就是 D_3 的作如此改变后的凯莱图．在这个用新的图象表示的群中，关系 $r^3 = f^2 = I$ 成立，但 $(rf)^2 = I$ 不成立．这个改变后的图形指出，$fr = rf$，即 $frf^{-1}r^{-1} = I$（从 I 到顶点 f 到顶点 fr，到顶点 r，再回到 I 的闭路）．这新的群是有关系

$$r^3 = f^2 = frf^{-1}r^{-1} = I$$

的阿贝尔群或交换群．因为它是用循环群 $C_2(f^2 = I)$ 与循环群 $C_3(r^3 = I)$ "组合"成的，所以我们用 $C_2 \times C_3$ 表示它．

练习 18　利用 $C_2 \times C_3$ 的凯莱图确定 fr 的逐次乘幂．对应于 $(fr)^6$ 的群元素是什么？证明 $C_2 \times C_3 = C_6$．（提示：设 $g = fr$，并指出每一个群元素都能表示成 g 的幂次．）

若改变二面体群 D_n 的图象中的一个 n 边形的边上的箭头方向，则我们得到有关系

$$r^n = f^2 = frf^{-1}r^{-1} = I$$

的"双重循环"群 $C_2 \times C_n$．类似地，由 D_∞ 的图象可得到无限"双重循环"群 $C_2 \times C_\infty$（见图 7.7）．此凯莱图象两条平行的单行街道，它们又被双行的纵向街道所连通．

考虑图 7.8 中的图象．看来它有点象单行街道网络，也

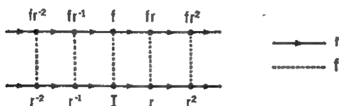


图 7.7

象一个城市的一部分地图. 在这个图象表示的群中，关系 $f^2=I$ 不成立，也就是说 f 的周期不是 2. 因此，我们在 f-线段上也画上了箭头. 指出可交换性的单一关系

$$frf^{-1}r^{-1}=I\ (\text{即 } fr=rf)$$

定义了这个群，这个单一关系反映在它的图象上，则是在每一个顶点存在一个对应于 $frf^{-1}r^{-1}$ 的矩形闭路. 这个"城市街道"群是两个生成元的更一般的阿贝尔群. (为了使群更一般，应从它的定义关系中删去某些限制，而仅仅留下限制 $fr=rf$.) 这个"城市街道"群用 $C_\infty\times C_\infty$ (或 C_∞^2) 表示.

群 $C_2\times C_3$ 称为循环群 C_2 与 C_3 的直积；类似地，$C_\infty\times$

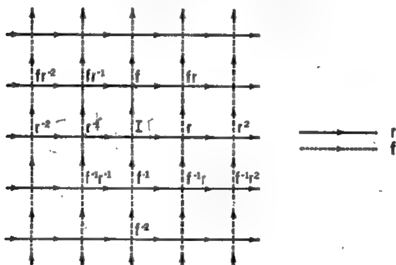


图 7.8

C_∞是C_∞与它自己的直积.直积这个概念的最一般最抽象的形式，是极其有用的；例如，可以指出，任何有限阿贝尔群是循环群的直积. 下面关于直积的讨论将是简要的，因而我们将依赖于例证来了解基本概念.

假设S是有二元运算$\otimes$的集合，群G和H是S的子集，且G和H都是以$\otimes$为运算的群. G有生成元$g_1, g_2, \cdots$，H有生成元$h_1, h_2, \cdots$. 我们规定G和H仅有单位元素是公共的，且G的任何元素与H的任何元素可交换. 在这些条件下，我们能用G和H的元素作为因子的乘积作成的集合来构造直积$G \times H$. 可以指出，集合$G \times H$是一个群，其生成元是$g_1, g_2, \cdots, h_1, h_2, \cdots$. ●

作为直积的一个例证，我们将考虑有生成元r和f的"城市街道"群(图 7.8)，有一个仅由r生成的无限循环群，还有一个仅由f生成的无限循环群. (应记住，在这些循环群的每一个中生成元都没有关系可满足.)这两个无限循环群除I外再无公同的元素. 若我们规定$rf = fr$ (或$rfr^{-1}f^{-1} = I$)，则第一个群的每一个元素与第二个群的每一个元素可交换，因而生成元r和f的集合生成直积$C_\infty \times C_\infty = C_\infty^2$.

直积与定义关系

一般地说，直积$G \times H$的定义关系集合，包含直因子群G和H的定义关系，及一个附加的等价于指定G的各生成元与H的各生成元可交换的关系. 附加关系保证G的每一个元素与H的每一个元素可交换，它是我们在直积的定义中所需要的. 现在我们来考虑一个是直积的群，并考察它的定义关系.

为了构造 $G = C_2 \times C_2$，我们从一个 2 阶循环群开始，

● 在我们的直积的例证中，集S将是群. 群G和H则是"群中群". 第八章将对这样的"子群"作系统的讨论.

它是用元素 x 生成的，且有关系 $x^2=I$；我们有另一个 2 阶循环群，它的生成元是 y 且有关系 $y^2=I$. 群 $G=C_2\times C_2$ 有两个生成元 x 和 y，满足两个关系 $x^2=y^2=I$. 指定 x 与 y 可交换可记为 $xyx^{-1}y^{-1}=I$，显然它等价于 $xy=yx$. 所以，$G=C_2\times C_2$ 是用直因子群的定义关系

$$x^2=I,\ y^2=I$$

及一个附加关系

$$xyx^{-1}y^{-1}=I$$

定义的. 因为 $x^{-1}=x$ 及 $y^{-1}=y$，所以我们能将 $C_2\times C_2$ 的定义关系写成

$$x^2=I,\ y^2=I,\ xyxy=I,$$

即

$$x^2=y^2=(xy)^2=I.$$

但是它们是 D_2（四群，见第 76 页）的定义关系，因此有 $C_2\times C_2=D_2$.

现在来考虑直积 $H=C_2\times D_2$. 假设 C_2 是元素 x 生成的，有关系 $x^2=I$；而 D_2 是元素 y 和 z 生成的，有关系 $y^2=z^2=(yz)^2=I$. 为了得到 $C_2\times D_2$ 的定义关系，我们还需在 C_2 和 D_2 的这些关系外再附加两个关系

$$xyx^{-1}y^{-1}=I,\ xzx^{-1}z^{-1}=I;$$

其中的第一个指定 x 与 y 可交换，第二个指定 x 与 z 可交换. 因为所有的生成元的周期都为 2，所以我们能将这两个附加关系写成

$$(xy)^2=I,\ (xz)^2=I,$$

从而对于 $C_2\times D_2$ 的全部定义关系集合如下

$$x^2=y^2=z^2=(yz)^2=(xy)^2=(xz)^2=I.$$

考虑图 7.9 中的 $C_2\times D_2$ 的图象表示，并观察这个图象的这样的某个部分，当取走其他无关部分时，它能解释成一个群的图象. 例如，图 7.10 中所示的部分就是四群的图象. 在

关于子群的下一章中，我们将指出"群中群"的意义。

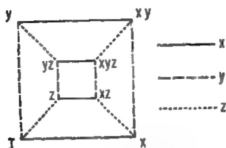


图 7.9

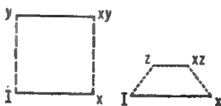


图 7.10

练习 19 求直积

(a) $G = C_2 \times C_4$ 及 (b) $H = C_3 \times C_3$

的定义关系集合及图象。

练习 20 利用凯莱图，乘法表或生成元关系来证明 $D_6 = C_2 \times D_3$。（一般地说，当 k 是奇整数时，$D_{2k} = C_2 \times D_k$ 都成立。）

练习 21 画一个被

$$a^2 = b^2 = (ab)^2$$

所定义的群的图象。［提示： 如有必要，首先证明或假设 $a^4 = b^4 = I$。］

练习 22 (a) H 是一个群，其生成元为 f 和 g，其定义关系为 $f^2 = g^2 = I$。画出这个群的图象。

(b) 回忆生成元为 r 和 f、定义关系为 $f^2 = (rf)^2 = I$ 的群 D_∞（见 78 页），证明 D_∞ 的定义关系的其他集合是 $f^2 = g^2 = I$，这里 $g = rf$。

第八章 子 群

对某些特殊群的内部结构的研究，将有助于深入了解它们的一些性质．某些群有一种内部结构，我们将用"子群"这个术语来刻划它．"子群"一词的含义也就是一个群中的群；也就是说，如果

(A) 集合H的每一个元素都是群G的一个元素，

(B)（关于G的二元运算）H是一个群，

则说集合H是群G的一个子群．这些条件的全部含义将在以下的讨论中逐步给出．我们从寻找并检验已给群的某些子群开始．

让我们考虑4阶循环群

$$C_4:\ I,\ a,\ a^2,\ a^3,$$

并找出它的2阶子群．因为子群是群，它必须包含元素I，所以下列集合都有资格作为群C_4中的2阶子群的候选者：

$$R=\{I,\ a\},\ S=\{I,\ a^2\},\ T=\{I,\ a^3\}.$$

首先我们承认，所有这些集合都满足条件(A)，这是因为这些集合的元素都是C_4中的元素．至于条件(B)则是有点担心的．我们注意，集合R包含两个元素，要能构成一个2阶子群只要$a^2=I$．然而，在C_4的二元运算下$a^2\neq I$．因此R不是C_4的一个子群．如果我们继续采用这种试探法，我们将求得，集合S是C_4仅有的一个2阶子群．我们应想出一个更简单、更系统化的试验方法．

为了证明一个集合在某个二元运算(例如⊗)下作成一个群，我们必须查明群的所有的公理都成立．如果从一开始我

们就已知道一个集合是一个群的子集，则检验公理的任务就变得比较简单了．为了看清这一点，让我们来查明定义子群的条件(B)．为此我们必须指出

(i) G的群运算$\otimes$限制于H的诸元素时是H的一个二元运算．

这相当于验证，若h_1及h_2是H的元素，则$h_1 \otimes h_2$在H中．当群G的一个子集有这个性质时，则我们说H关于$\otimes$是封闭的．(见4页关于封闭性的讨论．)为了证明H是一个群，我们还必须指出

(ii) 运算$\otimes$是可结合的，

(iii) H的各元素的逆元素在H中，

(iv) G的单位元素在H中．

条件(ii)是自动成立，这是因为在G中的群运算是可结合的．条件(i)和(iii)一起可推得条件(iv)；例如，若h是H的一个元素，则根据(iii)知h^{-1}在H中，再根据(i)知$h \otimes h^{-1} = I$在H中．所以，要使群G的一个子集H是一个子群只要如下两个条件成立即可：

(1) 当h_1和h_2在H中时$h_1 \otimes h_2$就在H中(封闭性)，

(2) 当h在H中时h^{-1}就在H中(逆元素)．

练习 23 证明上述命题等价于如下的断言：群G的一个子集H是G的一个子群，如果当a和b在H中时就有ab^{-1}在H中．(这个命题只包含一个条件．)

现在我们将利用条件(1)和(2)来确定C_4的子集R，S，T是否是一个子群．若一个集合不满足这些条件中的任何一个，则就不是一个子群．我们能用考察这些集合的乘法表来验证封闭性．(这时我们心中应记住，$a^4 = I$，$a^2 \neq I$，$a^3 \neq I$．)

集合 R

	I	a
I	I	a
a	a	a^2

集合 S

	I	a^2
I	I	a^2
a^2	a^2	I

集合 T

	I	a^3
I	I	a^3
a^3	a^3	$a^6=a^2$

表 8.1

只有集合 S 的乘法表关于群的运算是封闭的，也就是说，这个乘法表仅包含 S 的元素．如果集合 S 也满足条件(2)，则它将是子群；由 S 的乘法表一看就知，I 与 I 和 a^2 与 a^2 分别是互逆的．所以，S 的每一个元素的逆元素都在 S 中，因而 S 是 C_4 的一个子群．

C_4 有 3 阶子群吗？考虑包含 C_4 的单位元素 I 及其他任何二元素的集合；例如

$$D=\{I, a, a^3\}.$$

因为 $aa=a^2$ 是 D 的乘法表中的一个元素，但 a^2 不是 D 的元素，所以这个集合关于 C_4 的二元运算是不封闭的，因而不是一个群．读者很容易验证 C_4 的 3 个元素的其他集合也都不满足条件 (1)，所以 C_4 没有任何 3 阶子群．

每一个群都有两个特殊的子群．群 G 的所有元素组成的集合是 G 的一个子集，而且在 G 的二元运算下是一个群．所以任意群都是它自己的子群．由单一元素 I 组成的子集 H 也满足条件 (1) 和 (2)，这是因为 $I\otimes I=I$；所以每一个群都有一个仅由单一元素 I 组成的子群．

不是这两个特殊子群的子群叫真子群．通常我们的兴趣在于真子群．

练习 24 设 D_3 是 6 阶二面体群，其元素是

$$I, a, a^2, b, ba, ba^2,$$

其关系是 $a^3=b^2=(ba)^2=I$，

(a) 证明 $\{I, ba\}$ 是 D_3 的子群，

(b) 求一个 3 阶子群，

(c) 有 4 阶子群吗？

练习 25 设 C_5 是 5 阶循环群，确定 C_5 的所有真子群.

无限子群. 让我们来研究无限循环群 C_∞ 的子群. C_∞ 的生成元是 a，C_∞ 的元素是

$$\cdots, a^{-2}, a^{-1}, I, a, a^2, \cdots.$$

C_∞ 的任意子群都是循环群，这是因为它的每一个元素都是 a 的乘幂. 首先我们要问，C_∞ 有任何有限真子群吗？考虑子集

$$S_4 = \{I, a, a^2, a^3\},$$

初看起来，似乎 S_4 与 47 页讨论过的循环群 C_4 是相同的，然而在 C_∞ 的群运算下，在 S_4 中 $a^4 \neq I$；因此 S_4 不是群 C_4. 因为 a 的所有幂次在 C_∞ 中都是不同的，所以 S_4 在 C_∞ 的群运算下是不封闭的；例如，$a^2a^3 = a^5$ 就不在 S_4 中. 所以 S_4 不是 C_∞ 的子群. 同理可知，无限循环群 C_∞ 没有有限真子群.

C_∞ 有无限子群吗？集合

$$D = \{\cdots, a^{-4}, a^{-2}, I, a^2, a^4, \cdots\}$$

是用 C_∞ 的生成元 a 的偶次幂组成的. 因为任意两个 a 的偶次幂的乘积还是 a 的偶次幂，所以关于封闭性的条件 (1) 是满足的. 为了验证条件 (2)，观察 a^{2k} 的逆元素，是 a^{-2k}，它是 D 中的元素，所以 D 是 C_∞ 的子群. D 本身是用 a^2 生成的无限循环群. C_∞ 还有用 a^3，用 a^4 等等生成的子群. 所以 C_∞ 有无限多个真子群，它们的每一个都是一个无限循环群.

用普通加法作二元运算的、所有整数的无限循环群 N，是我们非常熟悉的. 在这个群中：

群元素——整数（正整数，负整数及 0），

群运算——普通加法，

单位元素——0，

a 的逆元素——$-a$，

生成元——1（或它的逆元素，-1）.

我们称这个群为(整数)加法循环群.

所有偶数的集合 E 是 N 的一个子群吗？我们来检验两个条件：

(1) 封闭性：任意两个偶数的和是偶数，

(2) 逆元素：任意偶数 k 的逆元素是 $-k$，它还是偶数，由于这两个条件都满足，所以所有偶数作成整数加法循环群的一个子群.

所有奇数的集合 O 是 N 的一个子群吗？任意两个奇数之和为偶数的事实证明，这个集合在加法下是不封闭的，所以奇数集 O 不是一个群.

练习 26 证明

(a) 所有 3 的倍数的集合作成整数加法循环群的一个子群；

(b) 所有 n（n 是任意整数）的倍数的集合作成加法循环群的一个子群.

练习 27 证明，若 R 和 S 是 G 的两个子群，则 R 和 S 的所有公共元素的集合是一个群(因而是 G 的一个子群).

练习 28 证明

(a) 所有复数 $a+ib$（a 和 b 是整数)的集合在加法运算下作成一个群；

(b) 当 r 和 s 是偶数时，所有形如 $r+is$ 的复数的集

合是(a)中的加法群的一个子群.

子群的阶 我们知道,"素数"是大于1的、除它自己和1外再无其他正因子的整数. 有趣的是,有些群也有类似的性质,即除它自己及仅包含单位元素 I 的两个子群外,这些群再无其他的真子群. 事实上,当且仅当某有限群的阶是素数时,这群才没有真子群. 这个断言的一部分("当"部分)是一个更一般的(指定有限群的阶与它的任意子群的阶之间的数值关系的)定理的推论. 这个定理(是1771年拉格朗日●阐述的)将在下面讨论.

拉格朗日是动力学领域中数学物理的伟大先驱者之一. 时至今日,人们仍用他的名字(Lagrange)的第一个字母"L"来表示动力学中的基本函数,以纪念他的贡献. 他在发展群论以及在解代数方程上的应用等方面的工作,也使人们难以忘怀. "拉格朗日预解式后来被伽罗华(Galois)开创性地应用群论来对代数方程的可解性进行研究. 现在我们回到关于有限群的子群的阶的拉格朗日定理的讨论.

拉格朗日定理 有限群的阶是其任意子群的阶的倍数.

这个定理断言,若 g 是群 G 的阶,而 h 是 G 的子群 H 的阶,则 $g=nh$,这里 n 是整数

$$1, 2, 3, \cdots, g$$

中的一个. 在特殊子群 G 及 I 的情况下,分别有 $n=1$ 及 $n=g$. 若 H 是此外的真子群,则 n 是整数

● 约瑟夫-路易斯·拉格朗日(1736—1813)创立了解决力学问题的强有力的数学方法,在他的解析力学论文中他以不用图形而自豪. 他由于在与月球运动有关的三体问题中应用他的方法而对天文学有所贡献. 寻找求解代数方程的一般方法的兴趣,使他成为看出群概念与方程的解之间的联系的第一个人.

$$2, 3, \cdots, g-1$$

中的一个.

在证明这个定理时，我们将利用陪集的概念，它是某些群元素的集合. 陪集这个概念在群论中是一个重要工具. 以下的简单引言将直接引出拉格朗日定理的证明.

群的陪集　设H是群G的一个子群. 为了表述的方便，假设H仅有4个(不同的)元素:

$$H = \{I, h_1, h_2, h_3\}.$$

假设b是G的元素但不是H的元素，考虑集合

$$H_b = \{b, bh_1, bh_2, bh_3\},$$

H_b 是用b左乘H的各元素得到的(我们指定左乘只是为了确定起见). 可以断言

(i) 集合H_b的所有的元素是不同的;

(ii) H与H_b没有公共的元素.

为了证明(i)，假设(例如) $bh_1 = bh_3$，在两边同时左乘b^{-1}，则得

$$b^{-1}bh_1 = b^{-1}bh_3 \quad 即 \quad h_1 = h_3.$$

这与H的4个元素是不同的假设矛盾.

为了证明(ii)，考虑H的某元素与H_b的某元素相等的可能性;例如假设$h_2 = bh_1$，则用h_1^{-1}右乘两边而有

$$h_2h_1^{-1} = bh_1h_1^{-1} = b,$$

因为H是群,所以元素$h_2h_1^{-1}$(即b)应在H中，但根据假设b不在H中. 所以H与H_b有公共元素的假设引出了矛盾.

所以G由8个元素构成，4个在

$$H = \{I, h_1, h_2, h_3\} \quad (G\text{ 的一个子群})$$

中,其他4个在

$$H_b = \{b, bh_1, bh_2, bh_3\} \quad (G\text{ 的元素的集合})$$

中．我们称 H_b 是群 G 的关于子群 H 的左陪集，记作

$$bH = \{b, bh_1, bh_2, bh_3\}.$$

子群 H 也是它自己的一个陪集，这是因为

$$H = IH = \{I, Ih_1, Ih_2, Ih_3\} = \{I, h_1, h_2, h_3\}.$$

若 c 是 G 的元素，但不是 H 和 H_b 的元素，则我们能用 c 得到关于 H 的另一个陪集：

$$cH = \{c, ch_1, ch_2, ch_3\}.$$

我们知道，陪集 cH 的元素是不同的，而且 H 与 cH 没有公共元素．我们可以断言，cH 的元素与 bH 的元素是不同的．这个断言的证明是练习 29 的解的一部分．所以 G 恰有 12 个元素，组成 3 个左陪集

$$H = \{I, h_1, h_2, h_3\},$$

$$bH = \{b, bh_1, bh_2, bh_3\}, \quad cH = \{c, ch_1, ch_2, ch_3\}.$$

若构成群 G 的元素恰有 12 个，则我们可将它们分解成互不相交的集合．我们用

$$G = H \cup bH \cup cH$$

来表示 G 是这些陪集的并集❶这个事实．

若 G 的元素多于 12 个，设 d 是不包含在 $H \cup bH \cup cH$ 中的任意一个元素，并作成另一个左陪集

$$dH = \{d, dh_1, dh_2, dh_3\}.$$

dH 的所有的元素是不同的，练习 29 的解指出，dH 与上述诸陪集的每一个都没有公共元素． 所以我们有 16 个不同元素构成 G 的元素，它们组成 4 个左陪集，每个 4 个．如果 G 只有这 16 个元素，则我们能记为

$$G = H \cup bH \cup cH \cup dH.$$

---

❶ 两个或更多个集合的并集，是原来这些集合的所有元素(共同的元素只取一次)组成的集合．

现在划分是清楚的．从阶为 h 的特殊子群 H 开始，我们能用这个子群外的一个元素 b 作成左陪集 bH，它有 h 个不同元素；这个左陪集与子群 H 合在一起共有 G 的 $2h$ 个不同元素．若有一个元素（例如 c）尚未计入，则我们可作另一个左陪集 cH，因而总共计入的 G 的不同元素共有 $3h$ 个．每次有 G 的(不在作成的诸陪集中的)一个元素，就可作成一个新的(附加 h 个不同元素的)左陪集．用这样的程序，每一步都增加 h 个不同的元素，因为 G 是有限阶的群，我们必然在某一步最终用完 G 的所有的元素．若作成关于 H 的 n 个左陪集以后，G 的所有元素全部用完，则我们将 G 分解成(每个都是 h 个元素的) n 个左陪集：

$$G = \underbrace{H \cup bH \cup cH \cup \cdots \cup kH}_{\text{每个都是 } h \text{ 个元素的 } n \text{ 个左陪集}}$$

所以，**G 的阶是 G 的任意一个子群 H 的阶的倍数**：用符号表示即 $g = nh$.

在群用(关于子群的)陪集概念表示的过程中，拉格朗日定理作为副产品被证明了．

练习 29　假设 rH 和 sH 是群 G 关于子群 H 的两个左陪集．证明 rH 与 sH 不是没有公共元素就是所有元素都是公共的．

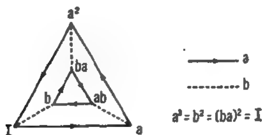


图　8.1

左陪集与右陪集的差别　拉格朗日定理的上述证明是利用左陪集进行的．如果我们利用右陪集进行证明，基本做法保持不变．其次我们要问，关于同一个子群的左陪集和右陪集，一般地说是否是相同的？如果不同，我们是否可要求任意一个左陪集(例如 bH)将恰好与某个右陪集(例如 Hc)有相同的元素？

考虑 6 阶二面体群 D_3(见图 8.1)．D_3 的一个子群是 2 阶循环群：

$$H:\ \{I,\ b\}.$$

我们将作 D_3 的关于 H 的左陪集和右陪集．(注意由图象看到 $a^2b = ba$ 及 $ba^2 = ab$)

左陪集	右陪集
$H = \{I,\ b\}$	$H = \{I,\ b\}$
$aH = \{a,\ ab\}$	$Ha = \{a,\ ba\}$
$a^2H = \{a^2,\ a^2b\} = \{a^2,\ ba\}$	$Ha^2 = \{a^2,\ ba^2\} = \{a^2,\ ab\}$

注意，在两种分解中除了 H 以外，没有两个陪集是相同的．陪集 aH 与 Ha 和 Ha^2 都不相同，而且 a^2H 也是如此．我们有二面体群 D_3 的两个不同的分解，分别分解成左陪集和右陪集．我们即可将 D_3 表示成(关于 H 的)左陪集的并集：

$$D_3 = H \cup aH \cup a^2H,$$

也可以将 D_3 表示成(关于 H 的)右陪集的并集：

$$D_3 = H \cup Ha \cup Ha^2.$$

这个例子指出，**群 G 的关于给定子群 H 的左陪集和右陪集可以得到 G 的不同的分解**．

无限陪集　我们已经看到，所有整数的集 N 用加法作二元运算时构成一个群(加法循环群)，所有偶数的集合 E 是它

的一个子群(88 页). 我们可以将 N 表示成关于子集 E 的陪集的并集. 做法与上述陪集的例子类似,设 a 是不在 E 中的一个元素,即设 a 是一个奇数,考虑用奇数 a 左"乘"(这里是左加) E 中的诸元素得到的集合 aE. 若 E 的元素是 $e_1, e_2, e_3, \cdots$, 则集合 aE 的元素是

$$a+e_1,\ a+e_2,\ a+e_3,\ \cdots.$$

因为一个奇数与一个偶数的和是奇数,又因为每一奇数都可以写成特殊的奇数 a 与某个偶数的和,所以陪集 aE 是所有奇数集 O,而且不论 a 选什么特殊的奇数,陪集 aE 都与集合 O 重合.显然陪集 E 和集合 O 正好用完集合 N,所以我们能写

$$N=E\cup aE,$$

即

$$N=\{\cdots,-2,0,2,\cdots\}\cup\{\cdots,-3,-1,1,3,\cdots\}.$$

(注意,因为群 N 是可交换的,其左陪集与右陪集是恒等的,所以 Ea 也是集合 O.)

子群 E 是所有 2 的倍数的集合;而陪集 aE 是所有除 2 余 1 的整数的集合. 能找到 N 的关于所有 3 的倍数的子群 T 的陪集的类似范型. 关于 T 的陪集是

$$\begin{aligned}T&=\{\cdots,-6,-3,0,3,6,\cdots\}\\&=\{\text{除 3 余 0 的所有整数}\},\\aT&=\{\cdots,-5,-2,1,4,7,\cdots\}\\&=\{\text{除 3 余 1 的所有整数}\},\\bT&=\{\cdots,-4,-1,2,5,8,\cdots\}\\&=\{\text{除 3 余 2 的所有整数}\},\end{aligned}$$

其中, a 是形如 $3n+1$ 的整数,而 b 是形如 $3n+2$ 的整数. 所以

$$N=T\cup aT\cup bT$$

是N的关于子群T的陪集表示.

练习 30 假设 rJ 和 cJ 是群 L 关于子群 J 的两个陪集，证明

(a) 若 c 是陪集 rJ 的任意一个元素，则

$$陪集\ cJ = 陪集\ rJ,$$

(b) 当且仅当 $r^{-1}c$ 是 J 的元素时才有

$$陪集\ cJ = 陪集\ rJ.$$

练习 31 证明，若

$$L = J \cup rJ \cup sJ \cup \cdots \cup vJ$$

是群 L 的关于子群 J 的左陪集表示，则

$$L = J \cup Jr^{-1} \cup Js^{-1} \cup \cdots \cup Jv^{-1}$$

是群 L 的一个右陪集表示.

练习 32 6阶二面群 D_3 的关于子群 $K = \{I, a, a^2\}$ 的左陪集和右陪集.

拉格朗日定理的某些结果 我们现在指出关于子群的阶的拉格朗日定理的某些容易得到的推论. 首先有

定理 4 若群G的阶是素数，则

(1) G没有真子群;

(2) G是一个循环群.

断言 (1) 由拉格朗日定理及素数的定义立即推得. 为了证明 (2), 我们用 r 表示素数阶 p 的群G的不是 I 的任意其他元素. 若 r 的周期是 n, 则 $r^n = I$, 且 $n > 1$, 集合

$$H = \{I, r, r^2, \cdots, r^{n-1}\} \quad (n-1>0)$$

构成G中一个 n 阶循环群(见练习 33), 所以H是给定的素数

阶 p 的群 G 的一个子群. 根据拉格朗日定理，它的阶 n 是 p 的一个因子. 因为 $n \neq 1$，所以必有 $n = p$，因此 H 是 p 阶子群，所以 H 是给定的群，这就证明了 (2).

我们必须认识到，拉格朗日定理仅指出，若群 G 的子群 H 存在，则 G 的阶必是 H 的阶的倍数. 拉格朗日定理的逆定理是否为真的问题，对我们来说暂时还是一个未解决的问题. 当 n 是 k 的倍数时，n 阶群必包含 k 阶子群吗？等到后面研究 12 阶四面体群的时候再回答这个问题.

在下列几个练习中将引出拉格朗日定理的一个有趣的推论. 读者做完这些练习后将得到费马 (Fermat) 小定理的证明，这个定理在数论中是很有名的.

练习 33 (a) 若群 G 的一元素 a 的周期为 n，则 $H = \{I, a, a^2, \cdots, a^{n-1}\}$ 是 G 的一个循环子群.

(b) 有限群的任意元素的周期与这个群的阶之间有什么关系?

练习 34 考虑用 $1, 2, \cdots, p-1$ 作元素的 (p 是素数)、用模 p 乘法作二元运算的 $p-1$ 阶"剩余类"群(见 24 页). 对于我们集合中的任意 2 个整数 x 和 y，有我们集合中的一个整数 r，使得 xy 与 r 被 p 除后有相同的余数，即有

$$xy \equiv r \pmod{p}.$$

显然，这个有限"剩余类"群的每一个元素都是有限周期的，假设 g 是周期为 n 的一个元素，

(a) 证明 $g^n - 1$ 是 p 的倍数，即证明

$$g^n - 1 \equiv 0 \pmod{p};$$

(b) 利用拉格朗日定理证明 $g^{p-1} - 1$ 是 p 的倍数，即证明 (见练习 33)

$$g^{p-1}-1\equiv 0 \pmod p.$$

练习 35 假设 a 是素数 p 的倍数；即有 $a\equiv 0(\bmod p)$，则 a^p 和 a^p-a 都是 p 的倍数，即有 $a^p\equiv a^p-a\equiv 0(\bmod p)$。证明即使正整数 a 不是 p 的倍数，就是说即使 $a\not\equiv 0(\bmod p)$，a^p-a 也是 p 的倍数。［提示：应用练习 34 的结果证明 $a(a^{p-1}-1)\equiv 0(\bmod p)$，即 $a^p-a\equiv 0(\bmod p)$。］这个练习的解证明了费马小定理：若 p 是一个素数，而 a 是任意正整数，则 a^p-a 是 p 的倍数。

练习 36 若 a 和 b 是群 G 的两个元素，证明

(a) ab 的周期等于 ba 的周期；

(b) 若 $ab=ba$，则 ab 的周期是 a 的周期与 b 的周期的乘积的因子；

(c) 若 $ab=ba$，m 是 a 的周期，n 是 b 的周期，则 ab 的周期恰好是 mn，且 m 与 n 互素（即 m 与 n 没有 1 以外的公因子）。

第九章 映　射

群的概念与映射(或映射集合)的概念关系非常密切. 现在我们通过考虑一些简单例子来引进这个概念（它已是大部分现代数学中的基本概念).

"映射"一词的通常含义是"作某物的映象". 作为数学的一个术语,"映射"的含义并未远离这个通常意义,这在数学中还是不多见的. 与此相反,通常的情况是,借用的词将给一个特殊的数学意义，与原来的意义相差甚远. 例如，群，域，环等,都是如此.

映射的数学概念是通常的城市地图的概念的一种很自然的抽象. 事实上，这样的地图是原来的对象(城市)在一张纸上的这样一种表示方法，原来对象(城市)的每一点在纸上有对应的一个(且仅有一个)点. 在各数学分支中，映射的数学概念从不偏离原来的元素与映象的元素之间的对应性这个基本概念.

我们想到的映射的一种简单情况是，映象是由有限个元素组成的集合，我们从这种简单情况开始. 假设我们有 3 个元素组成的集合 $X=\{a, b, c\}$ 和 $Y=\{r, s, t\}$. 我们能用各种方法将这两个集合的元素配对，例如

$$\begin{pmatrix} a & b & c \\ r & s & t \end{pmatrix}.$$

这里,元素间的对应是用一个在另一个的上面来表示的,每一个下面的元素与它上面的元素相对应. 这种对应性是一个集合 X 到另一个集合 Y 上的映射的一个例子. 一般地,由集合 X

到集合 Y 的映射是这样定义的：对集合 X 的每一个元素恰有集合 Y 的一个元素与之对应。

象上面那样的 X 到 Y 上的特殊的映射，可用如下一些不同方式表示（写成两行，外加圆括号）：

$$\begin{pmatrix} a & b & c \\ r & s & t \end{pmatrix} \text{或} \begin{pmatrix} a & c & b \\ r & t & s \end{pmatrix} \text{或} \begin{pmatrix} b & c & a \\ s & t & r \end{pmatrix}.$$

它们都表示 X 到 Y 上的同一个映射，这是因为在每一种表示中，集 X 的每一个元素都对应于集 Y 的相同的特殊元素，a 总是映为 r，b 映为 s，c 映为 t.

然而还有 X 到 Y 上的实质上不同的其他映射，例如

$$\begin{pmatrix} a & b & c \\ s & r & t \end{pmatrix}.$$

这个映射不同于前者，这是因为，虽然集 X 的元素 c 仍映到集 Y 的 t 上，但 a 已是映到 s 上而不是（前一映射的）r 上.

与（一集合到另一集合上的）映射概念有关的词汇及符号是各式各样的. 我们将需要其中的某些术语和符号，现在我们就来引进它们，希望读者通过这一章将逐步掌握它们.

已介绍的"两行-圆括号"只是映射的一种表示法，其他的表示法在本书中也出现过. 再看 33 页的关于群的二元运算的讨论时，我们就可看到，一个群的二元运算能看作是一个映射. 对群的每一个有序元素对 r 和 s，有群的唯一的元素 t 与其对应，使得

$$(r, s) \to t.$$

在这种方法中，群元素的有序对的集合映到这个群上. 群乘法表刻划这映射. 所有对 (r, s) 中的第一个元素写在第一列中，第二个元素写在顶上一行中，在这个映射下的 (r, s) 的象写在这个表中适当的地方.

当有一个由集合 X 到集合 Y 的映射时，我们记为 $X \to Y$.

我们也利用箭头表示个别元素间的对应；在我们的第一个例子中的映射可记为：$a \to r$，$b \to s$，$c \to t$. 在这个映射下，X的元素a对应于Y的元素r，这个r叫做a的象；类似地，s是b的象，t是c的象．集合X叫做这个映射的定义域，X的所有元素的象(是Y的元素)的集合，叫做这个映射的值域，也叫做X的象．

在本书中，我们将主要涉及这样一类特殊的映射，在这种映射中Y的每一元素都至少是X的一个元素的象，也就是说，X的象与集合Y重合．我们将说这样映射是映上（或X映到Y上）．上面给出的几个例子都是集合X映到集合Y上的．现在我们考虑由X到Y的映射

$$N: \begin{pmatrix} a & b & c \\ s & r & s \end{pmatrix}.$$

我们看到，N是一个映射，这是因为X的每一个元素都分别对应于Y的一个元素．但X不是映到Y上，因为Y的元素t不是X的任何元素的象．

由集合X到集合Y的映射也常常用一个符号（例如f）来表示，记为

$$f: X \to Y.$$

在这种表示法中，$f(a)=r$的含义即$a \to r$，也就是a的象是r. 类似地，b和c的象分别是$f(b)=s$，$f(c)=t$.

映射的概念也隐含在初等解析几何中，当我们构造一个二元方程的图象时就隐含地利用了一集合到另一集合的映射概念．例如，考虑方程

$$y = 2x + 1$$

和它的图象(见图9.1)．这个方程刻划了一个由X-轴到Y-轴上的映射，这是因为X-轴是这个映射的定义域，而整个Y-轴是其值域(或像集合)．这个映射可以表示成

$$f: x \to y \quad 或 \quad f(x) = y;$$

这个表示法含义是，x 的象是 y，其中 $y = 2x + 1$ 或 $f(x) = 2x + 1$。对 X-轴的每一个点，方程 $y = 2x + 1$ 恰对应于 Y-轴上的一点；也就是，每一个实数恰对应于实数作为它的象。例如，$x = 1$ 映到 $2 \cdot 1 + 1 = 3$ 上。

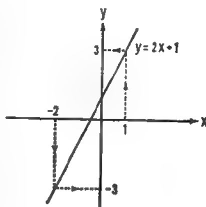


图 9.1

除一集合到另一集合上的映象外，也能将一集合映到它自己上。考虑集合 X: $\{a, b, c\}$，X 到它自己上的一种映射是

$$\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix};$$

这个映射将 X 的每一个元素都恰好对应于 X 的一个元素，这个映射的定义域与其值域是重合的。设用 M 来表示这个映射。

现在假设 a，b，c 是等边三角形的顶点，则这个映射这个三角形以过顶点 c 的高为轴所作的翻转，两个相继翻转是"映射 M 后再作一个映射 M"，两个相继映射可以表示成一个映射。

我们首先要问"映射 M 后再作一个映射 M"的含义是什

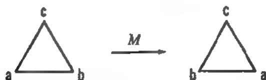


图 9.2

么？即

$$M^2=\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}=?$$

前面说过，一个映射可以写成各种两行-圆括号形式；例如M可以写成

$$\begin{pmatrix} b & a & c \\ a & b & c \end{pmatrix}.$$

注意这个括号中的上面一行与M的原来表示的下面一行是相同的。于是上面的问题又可写成

$$M^2=\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}\begin{pmatrix} b & a & c \\ a & b & c \end{pmatrix}=?$$

在第一个括号中我们有 $a\to b$，在第二个括号中跟随的是 $b\to a$，所以净效果是$a\to a$，也就是a映到它自己。类似地，$b\to a$ 并跟随 $a\to b$ 的净效果是 $b\to b$；最后 $c\to c$ 跟随 $c\to c$ 的净效果是 $c\to c$。因此我们有

$$M^2=\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}=\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}=I,$$

所以"M 跟随 M"是一个将每个元素变为它自己的映射，具有这种性质的映射叫做**恒等映射**，用 I 表示。

回到映射M的几何解释时，我们看到 M^2意味着绕过c的高作两次连续的翻转，其结果这个三角形返回到它的原来位置(见图 9.3)。

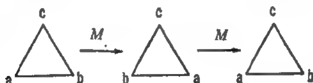


图 9.3

恒等映射的另一个例子是方程

$$y = x \text{ 或 } f(x) = x,$$

这个方程的图象(图 9.4)指出,每一个数都映到它自己.

作为群元素的映射 一个映射能作为一个映射集合中的一个元素来考虑.进一步,有一个恒等映射 I,而且我们将看到,两个映射的相继是一个映射.因此,可以断言,映射能作为一个群的元素.事实上,我们将作满足群公理的映射的某个集合.我们的讨论将限于集合到它自己上的映射.

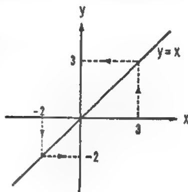


图 9.4

为了证明映射集合构成一群,除验证是否符合群公理外,别无他法.以前我们已这样做过多次,所以其一般程序我们是非常熟悉的.然而映射能用复杂的方式重新组合集合元素,我们应用有限经验着手验证时,应小心仔细点.

我们将首先证明"跟随"(或相继)是任意给定的集合 S 到它自己上的映射的集合上的二元运算.

(1) 二元运算:我们必须证明,若 M_1 和 M_2 是集合 S 到它自己上的两个映射,则乘积 M_1M_2 也是这样的映射.我们可将 M_1 和 M_2 简略地表示成

$$M_1 = \begin{pmatrix} a \cdots\cdots \\ b \cdots\cdots \end{pmatrix}, \quad M_2 = \begin{pmatrix} \cdots b \cdots \\ \cdots c \cdots \end{pmatrix},$$

其中 $a, b, c, \cdots$ 是给定集合 S 的元素.这第一个映射 M_1 将元素 a 映到元素 b,即 $a \to b$,这第二个映射 M_2 又将 b 映到

c，即 $b \to c$. 所以 M_1M_2 的净效果是 $a \to c$，因而 M_1M_2 是 S 的一个映射. 读者可用如下方法证明 M_1M_2 是映上的：若 y 是 S 的任意元素，则在映射 M_1M_2 下，存在 S 的一个元素 x 使得 $x \to y$.

(2) 结合性：初看起来，似乎我们的二元运算相继一定是可结合的. 然而因为在每次映射下，原来的集合都是重新改组的，在这样的条件下，映射的相继的可结合性不是显然的. 因此我们在这一点上应小心进行.

我们想要证明，对集合 S 到它自己上的任意 3 个映射 M_1，M_2 和 M_3 都有

$$(M_1M_2)M_3 = M_1(M_2M_3).$$

若 x 是 S 的任意元素，则 M_1 将 x 映到 S 的某个元素 y. 因为映射 M_2 和 M_3 也把 S 的每一个元素分别映到 S 的某一个元素，所以在 S 中存在元素 z 和 w，使得

$$M_1: x \to y,\ M_2: y \to z,\ M_3: z \to w.$$

所以 $(M_1M_2)M_3$ 的意义是 $x \to z$ 后再 $z \to w$，即 $x \to w$；而 $M_1(M_2M_3)$ 的意义是 $x \to y$ 后再 $y \to w$，即 $x \to w$. 所以 $(M_1M_2)M_3$ 及 $M_1(M_2M_3)$ 都是将 x 映到 S 的同一个元素上. 这就证明了可结合性.

(3) 单位元素：在恒等映射下，我们集合中的每一个元素都对应于它自己；即

$$I = \begin{pmatrix} a & b & c & \cdots \\ a & b & c & \cdots \end{pmatrix}.$$

显然，对于"接着"这种二元运算，这个映射是单位元素：

$$MI = IM = M.$$

（4）逆元素：考虑映射

$$M=\begin{pmatrix} u & v & w \\ r & s & t \end{pmatrix};$$

它的逆映射(记为 M^{-1})必须将M的值域的每一个元素返回到M的定义域中的元素上；换句话说，M^{-1}必须将每一个象遣送到原来的元素上．设

$$M^{-1}=\begin{pmatrix} r & s & t \\ u & v & w \end{pmatrix},$$

(注意，M^{-1}的行与M的行对换了)，则

$$MM^{-1}=\begin{pmatrix} u & v & w \\ r & s & t \end{pmatrix}\begin{pmatrix} r & s & t \\ u & v & w \end{pmatrix}=\begin{pmatrix} u & v & w \\ u & v & w \end{pmatrix}=I,$$

类似地有 $M^{-1}M=I$，所以 M^{-1} 是M的逆元素．

现在我们将指出，并不是每一个映射都有逆映射．例如，考虑映射

$$N=\begin{pmatrix} u & v & w \\ r & s & r \end{pmatrix}.$$

若它有一个逆映射(例如 X)，则X应将 $r\to u$, $s\to v$, $r\to w$，并使 $XN=NX=I$．但这不是一个映射，因为一个映射将定义域中的每一个元素只能对应于值域中的一个元素．但这里的X却将元素r对应于两个元u和w．因此映射N没有逆映射．

是什么原因造成映射M与映射N之间有这种差别：M有逆映射，而N没有？这是因为M将不同的元素映到不同的象上，而N的定义域中的两个不同的元素u和v却映到同一个象r上．一个映射有逆映射的充要条件，是它将不同的元素映到不同的象上，即它的值域的每一个元素仅对应于定义域中的一个元素．具有这种性质的映射叫一一映射或一对一映射，可简记为 1-1．

我们指出，一个集合到它自己上的所有的 1-1 映射的集合(关于相继或"接着"这种二元运算) 将满足群公理 (因而是一个群). 我们将在以下的置换群(或对称群)中遇到这种群的具体表示法.

关于逆映射的进一步注释 让我们考察由

$$y = 2x + 1 \quad 或 \quad f(x) = 2x + 1$$

定义的映射M: $x \to y$. $y = 2x + 1$ 的图象如图 9.1 (101 页) 所示. 它是一一映射吗? 假设 x_1 与 x_2 是不同的, 象点 $f(x_1) = y_1$ 与 $f(x_2) = y_2$ 也是不同的吗? 若它们的差 $y_1 - y_2$ 是 0, 则它们是不同的. 因为

$$y_1 - y_2 = (2x_1 + 1) - (2x_2 + 1) = 2(x_1 - x_2),$$

根据假设, x_1 与 x_2 是不同的, 所以上式的右边不是 0, 因而上式的左边也不是 0, 所以 y_1 与 y_2 也是不同的. 映射 M^{-1} 是存在的; 我们断言它是

$$M^{-1}:\ x = \frac{y-1}{2}.$$

为了验证这个断言, 我们首先按M的意义将 x 映到 $y(=2x+1)$ 上, 然后按 M^{-1} 的意义映它的象 y, 我们得到

$$MM^{-1}:\ \frac{(2x+1)-1}{2} = x,$$

即 MM^{-1} 映 x 到 x 上; 所以 $MM^{-1} = I$. 类似地 $M^{-1}M$ 映 y 到 y 上, 这是因为

$$2\,\frac{y-1}{2} + 1 = y;$$

所以 $M^{-1}M = I$.

现在我们考虑被

$$y = x^2 \quad 或 \quad f(x) = x^2$$

定义的映射 N: $x \to y$, 它的图象如图 9.5 所示. 这是一一映

射吗？假设 x_1 与 x_2 是不同的，即 $x_1-x_2\neq 0$，能推得

$$y_1-y_2=f(x_1)-f(x_2)\neq 0?$$

象的差 y_1-y_2 是

$$y_1-y_2=x_1^2-x_2^2=(x_1-x_2)(x_1+x_2),$$

由假设知 $x_1-x_2\neq 0$；但若 $x_1+x_2=0$，则 $y_1-y_2=0$。所以，即使 x_1 与 x_2 是不同的，y_1 与 y_2 也不见得就是不同的；例如，当 $x_1\neq 0$ 时，若 $x_1=-x_2$，则 $y_1=y_2$。所以 N 不是一一映射，因而它没有逆映象．然而，若从 N 的定义域中去掉整个负 X-轴(或整个正 X-轴)，则被

$$y=x^2\ (x\geqq 0)$$

定义的新映射 $\hat{N}$ 是一一映射，而且有逆映射(见图 9.6)．在它

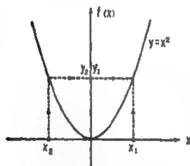


图 9.5

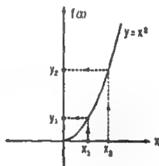


图 9.6

的受限制的定义域中，仅当 $x_1=x_2=0$ 时才有 $x_1=-x_2$ 成立，所以不同的元素映到不同的元素上．所以 $\hat{N}$ 是所有非负实数的集合到它自己上的一一映射．它的逆映射是

$$\hat{N}^{-1}:\ x=\sqrt{y}\ \ (y\geqq 0).$$

为了看出 $\hat{N}\hat{N}^{-1}=\hat{N}^{-1}\hat{N}=I$，我们注意 $\hat{N}\hat{N}^{-1}$ 是被

$$F(x)=\sqrt{x^2}=x(x\geqq 0)$$

给出的；而 $\hat{N}^{-1}\hat{N}$ 是被

$$G(x)=(\sqrt{y})^2=y\ \ (y\geqq 0)$$

给出的．

同态．现在我们回来考虑一个特殊类型的映射，它在群论的发展中有巨大的重要性．我们的兴趣将在叫做同态的一类映射以及它的特例——同构．与映射有关的这个概念不仅对研究群的性质有巨大价值，而且对研究其他的代数结构也是重要的．"同态"（homomorphism）及"同构"（isomorphism）这两个词都与结构有关，在英文中这一点是用词根"morph"显示的．

在给出同态的定义之前，我们先来看一个由整数加法群N到偶数加法群E（见 88 页）上的同态映射的例子．我们来考虑将N中的每个元素n与E中的元素$2n$对应的映射M：

$$M=\begin{pmatrix}\cdots, & -2, & -1, & 0, & 1, & 2, & \cdots\\ \cdots, & -4, & -2, & 0, & 2, & 4, & \cdots\end{pmatrix}.$$

我们看到，对N的任意两个元素n_1和n_2，$n_1\to 2n_1$，$n_2\to 2n_2$，从而$(n_1+n_2)\to 2(n_1+n_2)$；所以n_1与n_2的和的象$2(n_1+n_2)$是$2n_1+2n_2$，是n_1与n_2的象的和．读者应记住这个映射M，作为一个群到另一个群上的同态的具体例子．

现在我们假设有两个群G和H及一个G到H上的映射f．这也就是说，H的每一个元素是G中的某个元素的象．群G的元素a及b的象分别用$f(a)$及$f(b)$表示；当然，$f(a)$及$f(b)$都是H的元素．因为G和H是群，所以ab在G中，而$f(a)f(b)$在H中．

群G到群H上的同态映射的特征性质是，若a及b是G的元素，则群乘积ab映到H中的元素$f(a)f(b)$上；也就是说，两个元素的乘积的象是它们的象的乘积，用符号表示即

$$f(ab)=f(a)f(b).$$

在上面的例子中，群N是同态地映到群E上，每一个群的群运算都是加法:

$$f(n_1+n_2)=f(n_1)+f(n_2).$$

必须清楚地理解，一般地说，群G和H都有各自的特定的单位元、二元运算等. 所以

$$f(ab)=f(a)f(b)$$

只是下面的细致的表示方法的一种简略写法: 若$\otimes$表示群G的二元运算，$\boxtimes$表示群H的二元运算，而f是G到H上的同态映射，则对群G的任意两个元素a和b有

$$f(a\otimes b)=f(a)\boxtimes f(b).$$

但是，今后除非需要澄清，否则我们将不用这种精确表示法，而只简记为$f(ab)=f(a)f(b)$. 虽然群映射都是建立两个集合的个别元素之间的对应性，而一个群到其他群上的同态映射则特别考虑两个群所含的二元运算，并建立群乘积之间的以及个别元素之间的对应性.

作为同态映射的另一个例子，让我们考察一下C_4到C_2的下列映射$f: C_4\to C_2$:

$$\begin{pmatrix} I & a & a^2 & a^3 \\ I^* & b & I^* & b \end{pmatrix}.$$

注意，我们在C_2的单位元素上加了一个星号，星号在这里用来表示两个不同群的单位元素的区别. (至于两个群的二元运算之间的不同，我们已经在上面指出过.)今后，读者应记住这种区别的存在，即使标记，也不会如此精细.

从C_4的乘法表能验证，f将C_4元素的每一个群乘积映到这些元素的C_2中的象的乘积上;即

$$f(rs)=f(r)f(s),$$

其中r和s是C_4的两个任意元素. 在C_4的乘法表9.1中显示了每一个群乘积，而在这些群乘积下面的(等式)则是它们

	I	a	a^2	a^3
I	I $f(I)=I$	a $f(a)=b$	a^2 $f(a^2)=I$	a^3 $f(a^3)=b$
a	a $f(a)=b$	a^2 $f(a^2)=I$	a^3 $f(a^3)=b$	I $f(I)=I$
a^2	a^2 $f(a^2)=I$	a^3 $f(a^3)=b$	I $f(I)=I$	a $f(a)=b$
a^3	a^3 $f(a^3)=b$	I $f(I)=I$	a $f(a)=b$	a^2 $f(a^2)=I$

表 9.1

在C_2中的象.注意，C_4中的所有这些乘积的象是4个C_2的群乘法表(这在表 9.1 中已用双线分隔出来).

同态映射 f 显露出 C_4 与 C_2 在结构上的"相似性"，事实上，这样的映射的存在确实是因为有这样的"相似性"。如果我们试图构造 C_3 到 C_2 上的同构，我们将遇到无法克服的困难，因为这两个群缺乏结构上(允许有同态映射)所必须的"相似性".

练习 37 证明，若 f 是群 G 到群 H 上的一个映射，但它不将 G 的单位元素映到 H 的单位元素，则这个映射不是同态；反之，若 f 是一个 G 到 H 上的同态映射，则 $f(I)=I$.

练习 38 假设群 G 被 f 同态地映到群 H 上，证明若 x 是 G 的任意一元素(其逆元素为 x^{-1})，则

$$f(x^{-1})=[f(x)]^{-1};$$

也就是说，一个逆元素的同态象是这个象的逆元素。

练习 39 假设群 G 被 f 同态地映射到群 H 上，并且假设对 G 的两个特定元素 x 和 y 有 $f(x)=f(y)$，证明

$$f(xy^{-1})=f(x^{-1}y)=I.$$

练习 40 假设 f 是一个群到另一群上的同态映射，证明

(a) 若 $f(x)=I$ 及 $f(y)=I$，则 $f(xy)=I$。

(b) 若 $f(xy)=I$，则 $f(yx)=I$。

同构 上面给出的 C_4 到 C_2 上的同态映射不是一一映射；C_4 的两个不同元素 a 及 a^3 都映到 C_2 的 b 上（除非两个有限群有相同的阶，否则一个到另一个有限群上的映射不能是一一的.）当一个群到另一群上的同态映射也是一一映射时，则称之为**同构映射**或**同构**. 所以，群同构是一群到另一群上的、满足如下两个条件的映射：

1）对所有的 a 和 b，$f(ab)=f(a)f(b)$， （同态），

2）当且仅当 $a=b$ 时才有 $f(a)=f(b)$， （一一）.

我们将用两个例子(一个是有限群，另一个为无限群)来说明同构映射. 读者将看到，一群到另一群上的同构映射揭示这两个群的结构上的“同一性”；确实因为有结构“相同”的群，才存在一个到另一个群上的同构映射.

考虑元素是 $x^4-1=0$ 的 4 个根的群 H：

$$H: 1, i, -1, -i \quad (\text{其中 } i=\sqrt{-1}).$$

设 f 表示 C_4 到 H 上的如下的映射：

$$\begin{pmatrix} I & a & a^2 & a^3 \\ 1 & i & -1 & -i \end{pmatrix}.$$

	I	a	a^2	a^3
I	I	a	a^2	a^3
	1	i	-1	-1
a	a	a^2	a^3	I
	i	-1	$-$i	1
a^2	a^2	a^3	I	a
	-1	$-$i	1	i
a^3	a^3	I	a	a^2
	$-$i	1	i	-1

r
$f(r)$

表 9.2

我们直接看到 f 是一一映射；但 f 是同态映射吗？ 为了回答这个问题，我们来考察 C_4 的乘法表 9.2（在这个表中我们仍将乘积 r 的象 $f(r)$ 记在 r 的下面），并将 r 与它的在 H 中的象 $f(r)$ 相比较。

当记住 $i^2=-1$ 时，读者容易验证，象元素 $f(r)$ 作成群 H 的乘法表，所以有

$$f(rs)=f(r)f(s),$$

从而映射 f 除一一外，还是同态映象，所以 f 是同构映象。我们说群 C_4 与群 H 是同构的．如果从一个群到另一个群上有一个同构映象，则说这两个群是同构的。 从这个观点看，同构是两个群含有同样多的（结构）性质，这种情况我们称为"有相同结构"。

这两个同构群的图象如图 9.7 所示。 显然，除顶点及生成元的名称外，这两个同构群的图象是相同的。

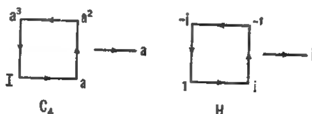


图 9.7

作为同构群的第二个例子，让我们考虑正实数集 P 和它的对数集 L(对数的特定的底并不重要,但为了确定起见，假设我们考虑的底是 10)。 首先我们指出,这两个集合都是群，它的二元运算等如下表所示:

	群 P	群 L
元素	正实数	正实数的对数(所有实数)
二元运算	普通乘法 ($x>0$ 及 $y>0$ 推得 $xy>0$)	普通加法 [$\log x+\log y=\log(xy)$]
单位元素	1	0
逆元素	倒数	负数

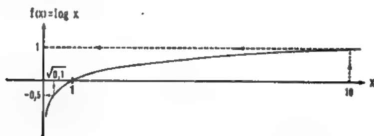


图 9.8

我们断言,这两个群是同构的,被

$$f(x)=\log x$$

给定的映射 $f:P\to L$ 是一个同构映射. 在这个映射下 L 的每

一个元素是P的某个元素的象，所以，所有正实数集是这个映射的定义域，而所有实数集是它的值域(见图 9.8)．尚须验证

(1) $f(xy)=f(x)f(y)$，对P的所有的x和y，

(2) 这个映射是一一的．

我们应小心区分群P与L的运算．设$\otimes$表示群P的二元运算，设$\boxtimes$表示群L的二元运算．则对P的任意二元素x及y，有

$$x\otimes y=xy \quad (\text{二个正实数的乘法});$$

而对L中的x与y的象$f(x)$及$f(y)$，则有

$$f(x)\boxtimes f(y)=\log x+\log y\ (\text{二实数的加法}).$$

因此，满足命题(1)的同态，需要对P的所有的元素x和y有

$$f(x\otimes y)=f(x)\boxtimes f(y)$$

即

$$\log(xy)=\log(x)+\log y.$$

但这个关系式是(关于乘积的对数的)熟知的定律；所以这个映射是所有正实数群到实数群的同态．

为了看出这个映射是一一的，我们仅需注意$f(x)=\log x$的图象．我们也能用指出两个不同元素总是映到两个不同元素来证明这个映射是一一的．假设$f(x)=f(y)$，即假设$\log x=\log y$，则

$$\log x-\log y=0,$$

即

$$\log\frac{x}{y}=0,$$

但$\log\frac{x}{y}=0$推得$\frac{x}{y}=1$，即$x=y$．所以这个映射是一一的，因而是同构．

抽象群 我们将说，两个同构的群是"抽象地相等"，也说

所有抽象相等的群是同一个抽象群. 所以今后我们可以说 6 阶二面体群, 或 6 阶循环群. "两个同构的群是抽象地相等"这个命题, 并不意味着这两个同构的群的各个具体细节都相同,而仅仅是说,这两个群有相同的结构上的群性质. 在练习 41 中我们将看到, 一个群与它的一个真子群同构是可能的. 一个群与它的一个真子群确实是不同的, 但仍可能有相同的结构.

可以指出, 对给定的阶 n, 仅存在有限个"抽象不同的"群. 含有 n 个不同符号的同一集合, 除元素的标记外, 仅存在有限个乘法表(表中共有 n^2 个值). 注意, 6 阶二面体群与 6 阶循环群是不同构的(因而是抽象不同的), 这是因为它们中的一个是不可交换的, 而另一个是可交换的. 除这两个群外, 不存在其他的抽象的 6 阶群. 类似地, 若 p 是任意素数, 则仅存在一个 p 阶循环群, 当然, 它是循环群 C_p.

假设不从这些例子出发, 读者也容易列举给定阶的不同的抽象群. 64 阶的不同的抽象群有 267 个, 但 256 阶的不同的抽象群一个也没有.

同构群的抽象识别, 类似于从特殊表示法中抽象出基数概念. 容易想到, 数 5 是 5 个元素 (5 个手指, 5 块美元, 5 个海洋, 5 个元音字母等等)组成的特殊集合的一种抽象. 同样地, 一个抽象群也能用各种特殊的表示法表示出来. 例如, 抽象的 4 阶循环群只有 1 个, 但却有许多具体表示法.

同构群(或抽象相等的群)的概念是重要的, 这是因为我们有时发现, 用某个具体表示法来证明群的定理不如用其他(同构的)表示来得容易. 因为同构群有相同的群结构, 所以只要证明了一个群, 定理就可推广到所有与它同构的其他群.

练习 41 一个群能同构于它的一个真子群吗？设 G 是整数加法群（见 14 页），设 H 是所有偶整数组成的、群 G 的(真)子群，证明 G 能同构地映到 H 上；即，若 x 和 y 是 G 的两个任意元素，则有一个 G 到 H 上的映射 f，使得

$$f(x+y)=f(x)+f(y)$$

及

$$f(x)=f(y) \quad \text{当且仅当} \quad x=y.$$

练习 42 将练习 41 的结果推广到抽象群 C_∞（见 48 页）．设 G 是用 r 生成的无限循环群，设 H 是用 $r^n(n>1)$ 生成的无限循环群(我们看到，H 是 G 的真子群)，证明 G 能同构地映到 H 上．

练习 43 设 G 是 r 生成的无限群，设 H 是 2 阶循环群，H 有元 I 及 b，且有 $b^2=I$，证明 G 能同态地映到 H 上，但不能同构地映到 H 上．

练习 44 设 G 是任意群，设 r 是 G 的任意确定的元素，如果 x 是 G 的任意元素，则 $r^{-1}xr$ 也是 G 的一个元素．我们用

$$f: x \to r^{-1}xr \quad (\text{即 } f(x)=r^{-1}xr)$$

定义 $f: G \to G$．证明 f 是 G 到它自己上的同构映射．

练习 45 设 G 是一个群，设 f 是使 G 的每一个元素映为其平方，即

$$f: x \to x^2 \quad (\text{或 } f(x)=x^2),$$

f 何时是一个同构映射(如果有的话)？

第十章 置换群

许多群论的文献中都讨论一类群，即所谓置换群或代换群．置换群特别有用是因为它给我们提供了所有的有限群的具体表示．在本章中，我们将看到：每个有限群都同构于某个置换群．

前面我们已经看到许多映射的例子中，把映射写成两行，定义域中的元素写在上面一行，而象元素写在下面一行．并且，我们已经证明，一个 n 个元素的集合到自己的一对一映射的全体所成的集合组成一个映射群．这种映射称为置换，而以置换为元素所构成的群就叫做置换群．

假设把三个元素的集合排成某个任意的但是确定的序列 a_1, a_2, a_3．为了方便，我们只要注意下指标，即把序列当成 1, 2, 3；这样一来，例如第三个元素 a_3，就可以简单地记作 3．

现在，设 M 是这个集合映到它自身上的某个一对一映射：

$$M: \begin{pmatrix} a_1, & a_2, & a_3 \\ a_2, & a_3, & a_1 \end{pmatrix} \text{或} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{或} \begin{matrix} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1. \end{matrix}$$

让我们把这个映射 M 解释为把序列 1, 2, 3 经过重排或置换而形成序列 2, 3, 1．这个解释就是把一个有限集合映到自身上的映射群称为置换群的根据．我们还可以把 M 看成把这个集合中的每一个元素代换成这个集合中的某个元素，在上面的例子中，1 换成 2，2 换成 3，3 换成 1．因此，把一个有限集合映到自身上的映射群在老的文献中常常叫做代换群．

置换表为循环❶映射，或者置换M表示对应这个循环图



这提示我们把M写成为单行的括号.

$$M:\ (1\,2\,3),$$

把这个记号解释为M把每个数字映到它右边的紧相邻的数字，这样到最后，把最右边的数字映到头一个数字，就完成了整个一个循环. M可以用三种方式写成循环，

$$(1\,2\,3),\ (2\,3\,1),\ (3\,1\,2),$$

因为在上面圆圈里面，把那一个元素写成头一个关系不大.

假如我们有一个四个元素a_1, a_2, a_3, a_4的集合的映射N:

$$N:\ \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 1 & 4\end{pmatrix}.$$

我们能否把这个映射表示成循环？因为4映到4，我们可以把N表示为

$$(1\,2\,3)$$

而把循环中不出现的任何元素理解为映到自身. 同样，

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 3 & 2\end{pmatrix}=(2\,4),$$

因为左边的映射可以完全用二项的循环来表示，而它可以读作$2\to4$, $4\to2$, $1\to1$, $3\to3$.

有限集合映到自身上的任何映射是否都能写成循环的形式？例如，我们怎样写映射

❶ 循环也可译成轮换——译者

$$A:\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 4 & 5 & 1 & 3\end{pmatrix}$$

它与上面的映射N不同，个别对应的集合不构成单一的循环图．让我们从1开始，把它的象2写在1的右边：

$$(1\ 2).$$

为了进一步扩大这个循环，我们看一下映射A中的对应就发现2的象是4．这样，扩大的循环就成为

$$(1\ 2\ 4).$$

如果我们想进一步扩大这个循环，我们看到，A把4映到1，于是完整的循环就是

$$(1\ 2\ 4).$$

但是，这个循环并不是映射A，因为它没有表达出来A所要求的把3映到5和把5映到3．而循环(3, 5)表示这件事，但它把其他元素都映到它们自己．因此，假如我们先作映射

$$(1\ 2\ 4)=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 4 & 3 & 1 & 5\end{pmatrix},$$

接着作映射

$$(3\ 5)=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 5 & 4 & 3\end{pmatrix},$$

显然其乘积就是A，即

$$(1\ 2\ 4)(3\ 5)=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 4 & 3 & 1 & 5\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 5 & 4 & 3\end{pmatrix}$$

$$=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 4 & 5 & 1 & 3\end{pmatrix}.$$

注意，因为这两个循环并没有公共的数字，所以谁也不影响谁．因此

$$(1\ 2\ 4)(3\ 5)=(3\ 5)(1\ 2\ 4).$$

我们把A表示为循环形式的办法可以用到有限集合映到

自身上的任何映射．因此，有限集合的任何置换可以写成无公共数字的循环的乘积．

让我们考虑映射

$$(1\,2)(2\,3) \text{ 及 } (2\,3)(1\,2),$$

考察一下有公共数字 2 的两个循环 (1 2) 及 (2 3) 是否可交换．(1 2) (2 3) 表示

$1 \to 2$ 接着 $2 \to 3$， 总结果是 $1 \to 3$，

$3 \to 3$ 接着 $3 \to 2$， 总结果是 $3 \to 2$，

$2 \to 1$ 接着 $1 \to 1$， 总结果是 $2 \to 1$．

因此，

$$(1\,2)(2\,3) = (1\,3\,2);$$

另一方面，(2 3) (1 2) 表示

$1 \to 1$ 接着 $1 \to 2$， 总结果是 $1 \to 2$，

$2 \to 3$ 接着 $3 \to 3$， 总结果是 $2 \to 3$，

$3 \to 2$ 接着 $2 \to 1$， 总结果是 $3 \to 1$，

因此，

$$(2\,3)(3\,1) = (1\,2\,3).$$

所以，这两个循环不可交换． 当循环没有公共数字时，它们的确可交换，但是，如果它们有公共数字时，它们可能不交换．

每一有限群都同构于一个置换群

上面几节提供了关于有限群的表示的基本定理的背景．在第九章中，我们指出任何特定的群都可以看成某个抽象群的许许多多可能的具体的表示中的一个，而这个抽象群同构于每一个表示．下面陈述的定理保证任何抽象有限群可具体表示为一个置换群． （回想 n 个元素的置换是 n 个元素的集合映到它自身上的一个一对一映射．）

定理 5 给定任意 n 阶有限群， 则存在 n 元素的置换群同构于这个群．

在有限群论的标准著作中都有这个定理的证明．在这里我们重复经典的证明还不如把这个定理应用于一个特殊群更使读者的认识深化．我们这里要用的方法可以推广成定理的一个正式的证明．

我们来求四阶循环群 C_4 的置换群表示．首先我们造 C_4 的乘法表，把元素 I，a，a^2，a^3 也分别表为 g_1，g_2，g_3，g_4．

	I / g_1	a / g_2	a^2 / g_3	a^3 / g_4	
I / g_1	I / g_1	a / g_2	a^2 / g_3	a^3 / g_4	$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=m_1$
a / g_2	a / g_2	a^2 / g_3	a^3 / g_4	I / g_1	$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=m_2$
a^2 / g_3	a^2 / g_3	a^3 / g_4	I / g_1	a / g_2	$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=m_3$
a^3 / g_4	a^3 / g_4	I / g_1	a / g_2	a^2 / g_3	$\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}=m_4$

表 10.1　C_4 的乘法表

表 10.1 中的每一行是第一行的置换(见定理 1，39 页)；例如，第二行的序列 g_2，g_3，g_4，g_1（或简化为 2，3，4，1）是第一行序列 1，2，3，4 的置换．表的右方表示这四个置换或一对一映射．它们可用循环写成

$$m_1=(1)(2)(3)(4)=I,$$
$$m_2=(1\,2\,3\,4),$$
$$m_3=(1\,3)(2\,4),$$
$$m_4=(1\,4\,3\,2),$$

（为了把 $m_1 = I$ 写成循环之乘积，我们引入一个数字的循环.）

练习 46 直接由循环来验证

(a) $m_2^2 = m_3$, (b) $m_3^2 = I$, (c) $m_2^3 = m_4$, (d) $m_2m_4 = I$, 以及映射 m_1, m_2, m_3, m_4 构成一个群 M.

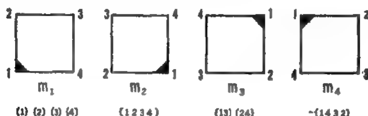


图 10.1

为了证明置换 m_1, m_2, m_3, m_4 构成的群M同构于 C_4，取正方形的四个顶点为按照映射 m_1, m_2, m_3, m_4 来进行重排的四个对象（见图 10.1）。显然，m_1 是置换群M的单位元素．把 m_1 与 C_4 的单位元素对应起来．置换 m_2 就等价于按反时针方向旋转 90°❶ 把 m_2 与 C_4 的生成元对应起来．

练习 47 把M的其余元素 m_3 及 m_4 映到 C_4 的元素，使得M同构映到 C_4 上．

读者可能想研究一下为什么表 10.1 中的映射构成一个

❶ 为看出 $m_2 = (1, 2, 3, 4)$ 对应于这个特殊的正方形按反时针方向旋转 90°，回忆一下 16～21 页上所讨论的重合运动．在那儿我们把转过的图形看成叠合在原来位置的图形之上（图 3.2）；表示顶点对应的箭头就翻译成“换成”（见 16 页）．因此，$m_2 = (1, 2, 3, 4)$ 表示 $1 \to 2$（1 换成 2），$2 \to 3$（2 换成 3），等等．于是，这个顶点具有特殊标记的正方形经 m_2 后的总结果就是使它从原来的位置按反时针方向旋转 90°．

与原来的群同构的群. 下面我们简要的叙述一下背景的想法. 四个映射 $m_j(j=1, 2, 3, 4)$ 可以写成

$$m_j: \begin{pmatrix} g_1 & g_2 & g_3 & g_4 \\ g_jg_1 & g_jg_2 & g_jg_3 & g_jg_4 \end{pmatrix},$$

也就是说, m_j 是映射

$$g_i \to g_jg_i \quad (i=1, 2, 3, 4),$$

映射 m_jm_k 表示映射 m_j 接着映射 m_k, 因此 m_jm_k 是映射

$$g_i \to g_jg_i \text{ 接着 } g_i \to g_kg_i,$$

因此, m_jm_k 是映射

$$g_i \to g_j(g_kg_i) = (g_jg_k)g_i.$$

所以, 置换群中的乘积 m_jm_k 与群 C_4 中的乘积 g_jg_k 的一对一对应. (与 39 页的定理 1 比较一下.)

下面我们求四群 D_2 的置换群表示. 见图 10.2 及表 10.2.

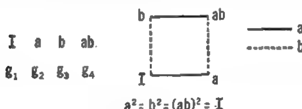


图 10.2

置换群M的元素表为双行-圆括号. 用循环表示就成

$$m_1 = (1)(2)(3)(4),$$
$$m_2 = (1\ 2)(3\ 4),$$
$$m_3 = (1\ 3)(2\ 4),$$
$$m_4 = (1\ 4)(2\ 3).$$

练习 48 (a) 对于群 M, 验证 $m_2^2 = m_3^2 = (m_2m_3)^2 = 1$.
(b) 用双行-圆括号描述置换群M到四群上的同构映射, 四群

	I g_1	a g_2	b g_3	ab g_4	
I g_1	I g_1	a g_2	b g_3	ab g_4	$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=m_1$
a g_2	a g_2	I g_1	ab g_4	b g_3	$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=m_2$
b g_3	b g_3	ab g_4	I g_1	a g_2	$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=m_3$
ab g_4	ab g_4	b g_3	a g_2	I g_1	$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}=m_4$

表10.2 D_2 的乘法表

具有元素 I, a, b, ab 及定义关系 $a^2=b^2=(ab)^2=I$.

正如上面的例子 C_4 的情形一样，用置换来表示四群也提供了一种基于四个对象的重排的具体解释．这一回，这四个对象是正四面体的四个顶点（见图 10.3）．置换 m_1 是单位元素，它把顶点保持在原来的位置上．置换 $m_2=(12)(3,4)$ 的作用是把顶点 1 和 2 互换，顶点 3 和 4 互换，见图 10.4．正四面体在映射 m_2 的作用结果就相当环绕如图 10.4 中的AB轴旋转180°，AB 轴通过两"对"边 1—2 及 3—4 的中点．我们把 AB 称为四面体的中线．同样 m_3 及 m_4 可以分别解释为环绕中线 CD 及 EF 旋转180°，见图 10.5．

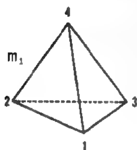


图 10.3

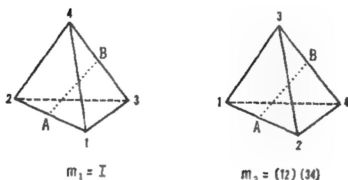


图 10.4

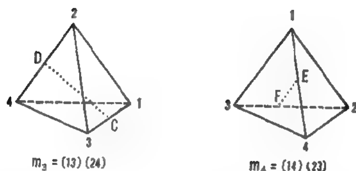


图 10.5

因此，四群的一种表示是一组特殊的运动，这运动是围绕中线旋转 180° 使得正四面体和自身重合. 能够证明：正四面体的三条中线交于一点并且互相垂直，因此四群也可以看成是把一组互相垂直的轴变到自身的一组转动所构成.

下一章我们将考察所有使正四面体叠合的运动所构成的四面体群，我们将会看到四群是四面体群的子群.

练习 49 (a) 造六个符号的置换群使之同构于 6 阶二面体群.

(b) 用循环来表示这个置换群的元素。

练习 50 已给六个元素：I, $a=(123)$, $b=(132)$, $c=(12)$, $d=(13)$, $e=(23)$. 证明它们组成 6 阶的二面体群. [提示：此处群的元素用三个符号的置换来表示，而在上面的练习中，它们用六个符号的置换来表示.]

四面体群

一组有趣而重要的群是与五种正多面体的重合运动群有关的群. 这五种正多面体是正四面体，立方体(正六面体)，正八面体，正十二面体及正二十面体. 要详细地讨论所有这些群就超出了本书的范围. 我们只限于简单地讨论(正)四面体群.

必须记住，正如所有的运动群一样，群的二元运算是相继或接着. (读者最好利用一个四面体的物理模型来帮助他想象下面所讲的运动.)

在讨论正四面体的重合运动群时，我们先数一下群的不同的元素数目，然后再挑出来生成整个群的基本运动. 我们的办法是推广我们早先研究等边三角形的重合运动的二面体群 D_3 的办法(29 页).

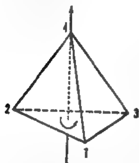


图 10.6

我们选取从顶点 4 到顶点 1, 2, 3 的三角形的顶垂线为一旋转轴，其方向如图 10.6 所示. 我们把轴的箭头看成是右手螺旋拧进的方向，而用 r 表示在拧紧螺丝的方向上转 120°. 假如围绕这个轴旋转四面体，在顶上的顶点 4 保持不动，我们可以得到三个不同的位置，在图 10.7 中标记为 I, r, r^2. 为了达到其他的位置使四面体同自身重合，我们需要考

虑把顶点 4 换成其余的三个顶点的运动. 因为对于四个顶点不管哪个在顶上,四面体都有三个位置,所以正四面体共有十二个不同的重合运动. 四面体群的阶数为 12.

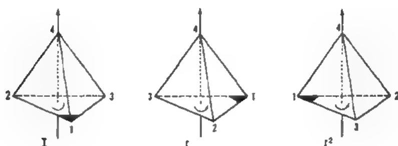


图 10.7

把顶上的一个顶点换成另一顶点的运动是围绕四面体的中线旋转 180°. 让我们用 f 表示围绕中线 AB 的翻转(或旋转 180°), 通过这个运动, 我们就到达图 10.8 所表示的新位置. (注意 f 把顶点对 2, 4 和 1, 3 互换.)图 10.9 表示运动 r 接着运动 f 的结果所到达的位置, 而图 10.10 表示 f 接着 r.

读者可以验证四面体的所有的重合运动都可通过把 r 及 f 结合起来而得到,也就是说, r 及 f 生成四面体群. 特别绕三条中线任何一个的翻转所到的位置可用 r 及 f 拼成的字表

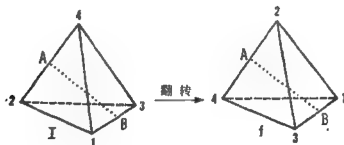


图 10.8

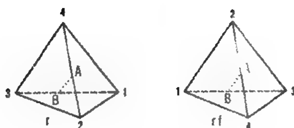


图 10.9

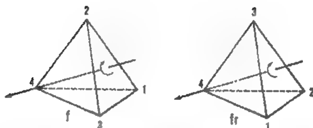


图 10.10

示. 但是，我们刚才已经看到这些运动组成四群的一个具体表示(126 页). 所以，四群是四面体群的一个子群.

生成元素 r 及 f 可以表示为四个顶点到自身上的映射:

$$r=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}=(123)=(12)(13),$$

$$f=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=(13)(24),$$

可以观察到，r 与 f 都是两个循环的乘积，其中每个循环只有两个符号. 现在我们还不能指出这个观察的全部意义，在后面讨论对称群及交代群的章节(158 页)中，我们要谈到这句话蕴含什么结果. 现在我们提一下，四面体群常叫做 A_4，A_4 表示四个符号的交代群.

四面体群 A_4 的图象.

我们用类似于画二面体群的图象的办法（见 58 页）来造 A_4 的图象.

考虑图 10.11a 中所示的截断四面体. 在每个顶点处的三角形可解释为代表周期为 3 的旋转. 在图 10.11b 中，我们把三角形的边用箭头标记来表示围绕四面体的某一固定顶点的转动. 当我们看到如何从重合运动的这种表示得出图象来时，就能验证三角形边所指定的特殊方向是正确的. 连结两个三角形的线段可以看成表示围绕中线的周期为 2 的翻转. 我们记得在群的图象中，周期为 2 的生成元用没有箭头的单线段表示，所以在图 10.11b 中，这些棱没有标上箭头.

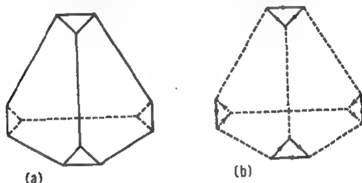
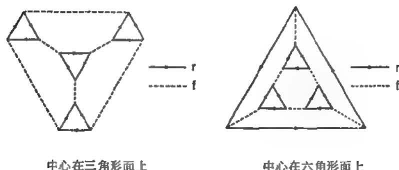


图 10.11



中心在三角形面上　　中心在六角形面上

图 10.12

我们看到截断四面体的面是三角形及六边形．为了得到一个二维表示，我们把四面体加以变形，使得其中心在一个三角形或一个六角形中，见图 10.12．在这些变形中，我们把对应于 120° 的旋转 r 的每个定向线段表为实线，而对应于周期为 2 的翻转 f 表为虚线．结果得出的网络是拓扑不变的．

我们断言，这些网络就是四面体群 A_4 的图象．对于读者来说，重要的是我们不能总是通过造出一个物理模型来表示重合运动来得出群的图象来，因此，我们不能自动地假定，这样得出的网络就是群的图象．在每一种情形下，我们必须检查这个网络来验证以前对于群的图象证明过的性质的确成立．

四面体群 A_4 的定义关系

第七章中，我们详细地讨论过二面体群 D_3 的定义关系．类似的论证说明：群 A_4 完全由下面的依据决定：

(1) A_4 由两个元素 r 及 f 生成；

(2) 这两个生成元满足三个定义关系：

$$r^3 = I,\ f^2 = I,\ rfrfrf = I\ [\text{或}\ (rf)^3 = I].$$

练习 51 读者可在 A_4 的图象上验证 $rfr^2 \cdot r^2fr = f$．利用定义关系 $r^3 = f^2 = (rf)^3 = I$ 证明 $rfr^2 \cdot r^2fr = f$．

这样就结束关于正四面体重合运动的讨论．读者在 154 页还可以找到关于立方体及八面体的群的简短论述．我们在附录中将讨论二十面体(及十二面体)群的某些特点．

第十一章　正　规　子　群

现在我们来研究一个群到另一个群上的同态映射，特别注意这映射在群的子群上的作用．在群论的发展及应用上，某些子群起着重要的作用．1830 年伽罗华● 在研究代数方程的根的性质的过程中，发现了这些特殊的群——所谓正规(或自共轭，或不变)子群．伽罗华证明，对于每个代数方程，都对应一个有限阶群，方程的根的性质就依赖于方程的群的正规子群的特征，也就是说，正规子群提供了决定其相关的代数方程的解的特征的基础．

现在，我们从两个观点来考察正规子群：(1) 同态映射，(2) 关于正规子群把群分解为陪集．我们将会看到这两种方法反映了同样的基本结构性质的不同方面．用第(1)个方法在于通过"计算"作出符合群的公理的群元素之间细致的关系．

$D_3: I, a, a^2, b, ba, ba^2$

$a^3 = b^2 = (ba)^2 = I$

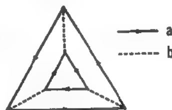


图　11.1

● 埃华瑞斯特·伽罗华(1811－1832)是一派数学方法的先驱，这派把数学的重点放在关于抽象结构的一般定理上．他利用这种方法发现并证明任何代数方程能用根式解的条件。他在这个工作中引进域的概念，并把域和群联系起来，他用的方法至今还作为"伽罗华理论"继续进行研究．伽罗华在 21 岁死于决斗．

我们已经作过这种计算,例如,解群方程并得出群的定义关系.

正规子群及同态映射

我们研究正规子群前先考察某些群同态. 我们要求这些同态把某些特殊的子群映到象群的单位元素上, 再看这种要求得到什么结果.

我们特别考虑 6 阶二面体群 D_3, 见图 11.1. 这群有一个子群 H: I, b. 假设 f 是 D_3 到 G 上的同态映射, 使得 H 的所有元素都映到象集的 I 上:

$$f(I) = I \text{ 且 } f(b) = I.$$

让我们考察一下 f 把 D_3 中不在 H 里的元素映到那里. 我们断言

$$f(a) = I.$$

为证明这点,我们写

$$a = Ia = (ba)^2 a = babaa \text{ 或 } a = (ba)(ba^2).$$

因为 f 是同态,对于任何群的元素 r 及 s,

$$f(rs) = f(r)f(s),$$

所以

$$\begin{aligned} f(a) &= f(ba \cdot ba^2) = f(ba)f(ba^2) \\ &= f(b)f(a)f(b)f(a^2) = f(a)f(a^2) \text{ (因 } f(b) = I) \\ &= f(a^3) = f(I) = I, \end{aligned}$$

这就是我们所断言的. 由此,

$$f(a^2) = f(a)f(a) = I,$$

$$f(ba) = f(b)f(a) = f(a) = I,$$

$$f(ba^2) = f(b)f(a^2) = f(a^2) = I,$$

所以 D_3 中每个元素都映到 I 上. 这就证明了, D_3 的任何同态映射,如把子群 H 映到 I 上,则把整个群 D_3 映到 I 上.

假设我们试另一个 D_3 到 G 上的映射 f, f 把另一个子

群，比如说K: I, a, a^2, 映到 I 上．由

$$f(I)=f(a)=f(a^2)=I$$

得出

$$f(ba)=f(b)f(a)=f(b),$$
$$f(ba^2)=f(b)f(a^2)=f(b),$$

于是，我们可以用

$$\begin{pmatrix} I & a & a^2 & b & ba & ba^2 \\ I & I & I & c & c & c \end{pmatrix}$$

来表示这个同态映射，其中 $c=f(b)$．因为

$$c^2=f(b)f(b)=f(b^2)=f(I)=I,$$

由元素 I 及 c 所成的集构成一个 2 阶循环群．● 因此，D_3 的同态映射如把子群K映到 I 上不非得把整个的 D_3 映到 I 上，而可能把群 D_3 映到 2 阶循环群上．

上述结果表明，D_3 的子群 H 及 K 之间有着本质的差别．我们将会看到，事实上有某种与子群K有关的性质不改变，与子群H相应的性质就发生改变．我们称K为**正规**或**不变**子群．发现一个正规（或不变）子群的本质属性的关键在于考察关于这个子群的陪集．

在第八章中，我们考察过一个群关于一个子群的陪集，并且列出 6 阶二面体群关于子群H的所有左陪集和右陪集．我们观察出陪集 aH 及 Ha 并不是相同的集（93 页），左陪集 aH 是集合

$$\{aI, ab\}=\{a, ba^2\},$$

而右陪集 Ha 是

$$\{Ia, ba\}=\{a, ba\},$$

那么 D_3关于 3 阶子群K的左、右陪集怎么样呢？它们是

● 这里我们默认这样的假定：$c=f(b)\neq I$．还存在（平凡的）映射 f，使得 $f(b)=I$；但是 $f(b)=I$ 不是 $f(a)=I$ 的必然推论．

左陪集　　　　　　　　　　右陪集

$K=\{I, a, a^2\}$　　　　　　$K=\{I, a, a^2\}$

$bK=\{b, ba, ba^2\}$，$Kb=\{b, ab, a^2b\}=\{b, ba^2, ba\}$.

关于K的左、右陪集完全一样，也就是$bK=Kb$.

D_3到2阶循环群上的同态映射有如下结果：

陪集$K\to I$，陪集$bK=$陪集$Kb\to f(b)$.

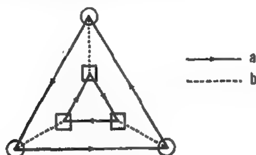


图 11.2

在图11.2中，二面体群D_3中的某个元素如果属于陪集K，则表成○，如果属于陪集bK，则表成□。在图11.3中，D_3关于子群H的左、右陪集也标记出来.

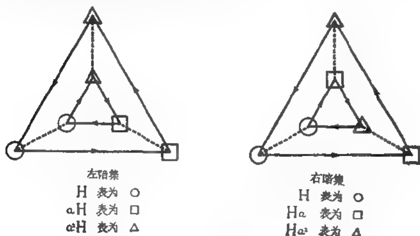


图 11.3

从这个例子可以看出 D_3 表为关于 K 的陪集的并的表示，不管是表为左陪集还是右陪集，是不变的.

一般我们把群 G 的子群 K 称为不变子群或正规子群，如果它具有性质：G 关于 K 的左陪集与右陪集相同. 注意，特别当 K 是只包含一个元素 I 的子群是正规子群，因为对于 G 中任何元素 g，陪集 gI 与 Ig 相同，每个都含有一个元素 g. 整个群 G 也是它自身的正规子群，这是因为任何左陪集包括 G 的所有元素，右陪集 Gg 也是一样.

下述定理表示不变子群与同态映射之间的本质关系.

定理 6 设 f 为由群 G 到群 H 上的同态映射，则 G 中满足 $f(x)=I$（其中 I 是 H 的单位元素）的所有元素 x 的集合 K 是 G 的正规子群.

在证明定理之前，我们要提一下，它为我们提供一种方法来检验群 G 的元素 x 不可能是与整个群 G 不同的正规子群的元素. 我们只须研究一下假定存在同态映射 f 使得 $f(x)=I$ 能得出什么推论. 假如由 $f(x)=I$ 推出 f 把所有元素映到 I 上，那么 x 就不是一个真正规子群的元素.

定理 6 的证明. 首先我们证明 K 是 G 的子群. 这只要证明子群的两个试验条件成立（85 页）；然后证明 K 是正规子群.

(1) 封闭性. 为了证明，假如 x_1 及 x_2 是 K 中任何两个元素，则 x_1x_2 也属于 K，我们来证明，由 $f(x_1)=I$ 及 $f(x_2)=I$ 可推出 $f(x_1x_2)=I$. 因为 f 是同态，所以

$$f(x_1x_2)=f(x_1)f(x_2)=I\cdot I=I.$$

这就证明 K 的封闭性.

(2) 逆元素. 我们证明，如 x 属于 K，则其逆元素 x^{-1} 也属于 K，即如 $f(x)=I$，则 $f(x^{-1})=I$. 因为 f 是同态，$f(I)=I$（见 111 页，练习 39），且

$$f(x^{-1}) = I \cdot f(x^{-1}) = f(x)f(x^{-1}) = f(xx^{-1})$$
$$= f(I) = I.$$
从而逆元素的条件满足.

现在，为了证明子群K是G的正规子群，我们必须证明，如y是G的任何元素，则$yK = Ky$.（记住我们的群G的正规子群的定义要求左陪集等于右陪集.）

命x_1为K的任意确定的元素，则x_1y是陪集
$$Ky = \{x_1y, x_2y, x_3y, \cdots\}$$
中的元素．为了证明x_1y是陪集
$$yK = \{yx_1, yx_2, yx_3, \cdots\}$$
中的元素，我们解方程
$$yz = x_1y$$
求出y并证明z是K的元素．这个方程的解是
$$z = y^{-1}x_1y,$$
且如果$f(z) = I$，则z属于K．但是，
$$\begin{aligned} f(z) &= f(y^{-1}x_1y) \\ &= f(y^{-1})f(x_1)f(y) && \text{(同态)} \\ &= f(y^{-1})f(y) && \text{(因 } x_1 \text{ 属于 } K\text{)} \\ &= f(y^{-1}y) && \text{(同态)} \\ &= f(I) = I. \end{aligned}$$
从而$z = y^{-1}x_1y$是K的元素．因为x_1y是陪集Ky的任意元素，所以我们已经证明Ky的每个元素都属于陪集yK.

同样，如yx_1是陪集yK的任意元素，我们能够证明yx_1是Ky的元素．我们只须要解方程$zy = yx_1$求出z，然后证明$z = yx_1y^{-1}$是K的元素．这就推出yK的每个元素都在陪集Ky中．于是$yK = Ky$.

阿贝尔群的子群是正规子群　设K是群G的正规子群．$yK = Ky$这种关系的外表就提示我们是讨论某种形式的交

换性质. 事实上, 我们所说的性质是, 对于K的任何元素x_1, 我们可以求出K的元素x_2使得

$$yx_2 = x_1 y \text{ 或 } x_2 = y^{-1}x_1 y \text{ 且 } x_1 = yx_2y^{-1},$$

其中y是G的任意元素. 由这个性质, 我们推出阿贝尔群或交换群的任意子群都是正规子群, 因为在阿贝尔群中, 对于群中任意两个元素, 有

$$yx_1 = x_1 y,$$

从而有$yK = Ky$.

练习 52 证明: 如群G是$2n$阶, n是整数, H是G的n阶子群, 则H是G的正规子群.

练习 53 假设群G的元素是$g_1, g_2, g_3, \cdots$. 命x表示其中之一, 并考虑集合

$$S = \{xg_1x^{-1}, xg_2x^{-1}, xg_3x^{-1}, \cdots\}.$$

证明, 集合S包含G的所有元素. (元素xg_1x^{-1}称为g_1关于x的共轭.)

练习 54 如x, y是群的元素, 满足$x = yxy^{-1}$, 则x, y必定满足什么关系? (我们称x关于y自共轭.)

练习 55 设K是G的正规子群, K的元素是$k_1, k_2, k_3, \cdots$. 命g为G中任何元素. 考虑集合$S = \{gk_1g^{-1}, gk_2g^{-1}, gk_3g^{-1}, \cdots\}$. 证明$S$与$K$是相同的集合. (我们把这个结果说成是正规子群是自共轭的.)

定理 6 的逆定理(商群) 当一个数学家完全证明了一个定理, 他自然而然面对着一个新问题: 这个定理的逆定理也

对吗？对于定理 6 来说，这个问题的答案还带来没有想到的奖赏，因为它“创造出”一种新型的群叫作商群．我们现在表述定理 6 的逆定理．

定理 7　任给群 G 的正规子群 K，存在一个群 H 及一个从 G 到 H 上的同态映射 f，使得 K 的元素恰好是 G 映到 H 的单位元素上的那些元素．

下一小节中，我们通过真正构造一群证明群 H 的“存在”，它与 G 和 K 的关系正如定理 7 所表述的一样．我们把这个群称为 G 关于 K 的商群(或因子群)，并用 G/K 表示．我们将看到 G/K 的元素是元素的集合，即 K 在 G 中的陪集．

商群

埃华瑞斯特·伽罗华首次证明：群 G 关于 G 的正规子群 K 的陪集构成一个群．这个群叫作商群 G/K．在我们研究这个群的过程中，我们必须适应这个新的事实，即我们这个群的元素本身是另外的群的元素的集合．

在我们证明伽罗华这个著名结果之前，我们必须在 G 关于其正规子群 K 的陪集的集合中定义一个二元运算．我们定义二个陪集 R 及 S (以这个顺序)的乘积为所有形如 rs (以这个顺序)的群乘积的集合，其中 r 是集合 R 中的元素，s 是集合 S 中的元素．从而，两陪集的乘积 $R \cdot S$ 就是包含在乘法表中的所有这种乘积的集合，其第一个因子取作 R 的元素，第二个因子取作 S 的元素．读者应该能证明，如 R 及 S 是 G 关于正规子群 K 的陪集，则 $R \cdot S$ 也是 G 关于 K 的陪集，也就是说，这种构成陪集的乘积的作法在 G 关于 K 的陪集的集合上定义一个二元运算．

现在我们利用我们所熟悉的二面体群 D_3 关于不变子群 K（三阶循环群）的陪集来阐明这个定义（见 134 页）．K 的陪集是

$$K:\ I,\ a,\ a^2 \ \text{及}\ \ bK:\ b,\ ba,\ ba^2.$$

假如我们根据定义来作乘积 $K\cdot K$，结果就得到出现在乘法表 11.1 中的所有元素的集合．乘积的集合显然是陪集 K；因此 $K\cdot K = K$．假如我们作乘积 $K\cdot bK$，我们就得到出现在乘法表 11.2 中所有元素的集合．读者用群 D_3 的图象作为乘

$K\cdot K$

	I	a	a^2
I	I	a	a^2
a	a	a^2	I
a^2	a^2	I	a

表 11.1

$K\cdot bK$

	b	ba	ba^2
I	b	ba	ba^2
a	ab	aba	aba^2
a^2	$a^2 ba$	$a^2 b$	$a^2 ba^2$

表 11.2

法表的方便办法能够验证，这九个乘积的集合与陪集 bK 重合，即 $K\cdot bK = bK$．同样，读者能够验证 $bK\cdot K = bK$，以及 $bK\cdot bK = K$．因此，任何两个陪集的乘积还是一个陪集，且 K 是单位元素．

	K	bK
K	K	bK
bK	bK	K

表 11.3

陪集 K 及 bK 的乘法表 11.3 总结了我们的结果．它表明，这两个陪集构成一个二阶循环群，而陪集 K 是单位元素．这个陪集的群 D_3/K 称为 D_3 关于 K 的商群（或因子群）．读者可以验证，由

$$x \to xK$$

定义的 $D_3 \to D_3/K$ 的映射是 D_3 到 D_3/K 上的同态映射. (证明 $xy \to xyK = xK \cdot yK$.)

"因子群"这个名称及 D_3/K 的记法来自把 D_3 唯一表示为关于 K 的陪集的并集

$$D_3 = K \cup bK$$

类似于因子分解. "仿佛"我们有

$$D_3 = (I + b)K = IK + bK = K + bK.$$

一般来说, 如果一个群 L 表示为关于正规子群 J 的陪集的并集

$$L = J \cup rJ \cup sJ \cup \cdots \cup vJ,$$

则这些陪集构成商群, 记为 L/J. 这个商群由这两个群 L 及 J 唯一决定.

练习 56 根据陪集乘积的作法作出一个群 G 的两个子群 R 及 S 的乘积. 证明

(a) 集合 $R \cdot S$ 是一个子群当且仅当 $R \cdot S = S \cdot R$;

(b) 如 R 或 S 中有一个是正规子群, 则 $R \cdot S = S \cdot R$ 是一个子群.

群的关系及商群

我们现在用群的关系及群的图象来表示这些关于正规子群, 同态映射及商群的结果.

图 11.4 表明二面体群 D_3 的图象. 商群 D_3/K 只有两个元素

$$K:\{I, a, a^2\} \text{ 及 } bK:\{b, ba, ba^2\},$$

而 D_3 有六个元素在群的图象中表为顶点. 假如我们把关系

$$a = I$$

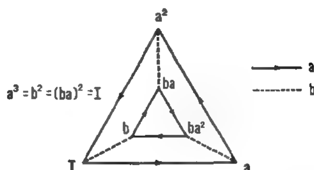


图 11.4

加到 D_3 的定义关系中去，K 及 bK 中的元素就成了

$$\{I,\ a=I,\ a^2=I\}\text{ 及 }\{b,\ bI=b,\ bI=b\},$$

因此，我们不仅得出子群 K 的所有元素成为元素 I，而且得出陪集 bK 的所有元素成为元素 b. 换句话说，附加的关系 $a=I$ 的效果就是把 K 中所有元素都团成一个元素 I，把 bK 中的所有元素都团成一个元素 b. 因为 $b^2=I$，附加的关系就得出一个 2 阶循环群，即同构于 D_3/K 的群. 因此，我们可以把引进关系 $a=I$ 看成等价于 D_3 到 D_3/K 上的同态映射，使得 K 的元素恰巧映到商群的单位元素上.

引进关系 $a=I$ 可表示为群网络的一种变形，它使对应于 K 的元素的顶点真正吸收在对应 I 的顶点上. 这个过程可以想象成把生成元 a "缩"成一点. 假如我们先把图象的形状改变成三维形式，然后把 a-线段"缩"成一点就更容易看清

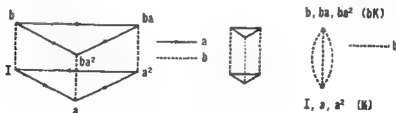


图 11.5

楚. 图 11.5 表示由左到右一个接一个地变形. 我们看到, 加进关系 $a = I$ (也即把正规子群映到 D_3/K 的单位元素上), 群 D_3 的图象成为 2 阶循环群的三重图象, 其中一个顶点对应于陪集 K, 另一个顶点对应于陪集 bK. 这样我们就通过 D_3 的图象的变形得出商群 D_3/K 的图象表示, 如图 11.6 所示.



图 11.6

让我们看一看, 对于无限群这些结果在多大程度上也对. 我们考察一下所有整数的加法循环群 N, 而把所有偶数的集合 E 作为它的正规子群. 我们已经把 N 表为关于正规子群 E 的陪集的并集, 即

$$N = E \cup aE \quad (a \text{ 不是 } E \text{ 中的元素});$$

见 94 页. (注意, 我们能够肯定 E 是 N 的正规子群, 因为一个阿贝尔群或交换群的任何子群都是正规子群.) 陪集 aE 是所有奇数的集合 O, 所以我们能够写成

$$N = E \cup O.$$

陪集 E 与 O 构成群吗? 我们必须确认

$$E \cdot E, \quad E \cdot O, \quad O \cdot E, \quad O \cdot O$$

这四个乘积中的每一个或是陪集 E 或是陪集 O, 并且群的公理成立. 记住群 N 的二元运算是加法, 我们得出:

$E \cdot E = E$, 因为 $E \cdot E$ 是两个偶数的所有和数的集合;

$E \cdot O = O$, 因为 $E \cdot O$ 是一个偶数和一个奇数的所有和数的集合;

$O \cdot E = O$, 因为 $O \cdot E$ 是一个奇数和一个偶数的所有和数的集合;

$O \cdot O = E$, 因为 $O \cdot O$ 是两个奇数的所有和数的集合.

表 11.4 是陪集 E 与 O 的乘法表. 因此, 商群 N/E 的乘法表

就是以 E 为单位元素的 2 阶循环群的乘法表. 第八章中，我们已看到无限循环群没有有限群为其子群；我们现在看到一个有限群可以是无限循环群的商群.

	P	Q
P	P	Q
Q	Q	P

表 11.4

下面我们仿照上面的例子的格式来造商群 N/E，也就是利用 N 的图(图 11.7)并加进一个关系等价于把正规子群 E 映到 I 上.



图 11.7

如果我们用 a 表示群的生成元，并添加关系

$$a^2 = I,$$

则

$$a^{-2} = I,\ a^4 = I,\ a^{-4} = I,\ a^6 = I,\ \text{等等}.$$

这个添加的关系所起的作用就是把所有 a 的偶次幂映到 I 上；换句话说，加法循环群 E 映到 I 上. 由这组扩大的关系定义的群正好就是 2 阶循环群，这就是商群 N/E. (我们刚才谈到把一个关系加到"原来"一组关系上，这是为了保持上面 D_3 的例子的格式. 但是，现在这个"原来"一组关系是空的；C_∞ 是自由群，见 63 页.)

把 E 中所有元素映到 I 上对于 N 的图象有什么影响呢？为了回答这个问题，我们把图象加以变形，把对应于 E 中元素

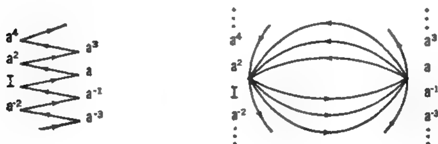


图 11.8

的顶点吸收到对应于 I 的顶点中去，其余对应于陪集 O 中的元素的顶点也吸收到一点中去(见图 11.8)．经过这种作法之后，N 的图象就成为 2 阶循环群的无限重的图象，其中一个顶点对应于陪集 E，另一个顶点对应于陪集 O．图 11.9 表示商群 N/E 的图象．



图 11.9

假如，我们不添加关系 $a^2=I$，而添加关系 $a^3=I$，其结果将是把所有 3 的倍数的子群映到 I 上．图 11.10 表示已变形的图象以及对应于 T 的顶点最后吸收进对应 I 的顶点中去．结果得到的是商群 N/T 的图象．

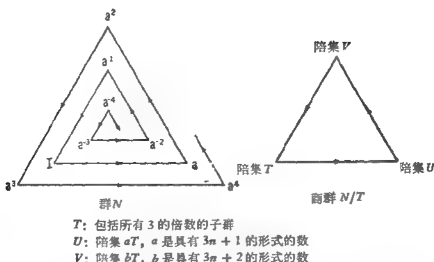
从我们对 D_3 及 N 的讨论可得出下面的格式：

(1) 我们考虑一个群 G 有已知的生成元及定义关系．

(2) 引入一个新关系；也就是令由 G 的生成元所成的某一个字等于 I．

(3) 这个新关系现在使 G 的另外一些元素也等于 I．由新关系及群的公理所有等于 I 的元素的集合构成 G 的一个正规子群 K．

(4) 结合 (1) 与 (2) 的关系定义商群 G/K．



T: 包括所有3的倍数的子群
U: 陪集aT, a是具有$3n+1$的形式的数
V: 陪集bT, b是具有$3n+2$的形式的数

图 11.10

这是我们通过同态映射变通我们处理商群G/K的办法，因为(2)及(3)一起等价于G到商群G/K上的同态映射使得正规子群K的元素正好都映到I上.

我们可以推广这个格式如下:

(1) 考虑一个群具有已知生成元及n个定义关系

$$R_1=I, R_2=I, \cdots, R_n=I.$$

(2) 通过由G的生成元构成的字等于I，引进s个附加的关系

$$R_{n+1}=I, R_{n+2}=I, \cdots, R_{n+s}=I.$$

(3) 由新关系及群公理得出的群G中等于I的所有元素形成G的一个正规子群K.

(4) 这$n+s$个关系

$$R_1=I, R_2=I, \cdots, R_{n+s}=I$$

定义商群G/K.

我们不准备给出这些断言的全部证明. 我们仅仅指出，为什么添加新关系等价于定义G的正规子群K。我们首先考

察一下添加一个新关系（比如说 $R_{n+1}=I$）的直接结果而产生的等于 I 的 G 中的元素. 因为 R_{n+1} 是 G 的生成元的一个字，所以 R_{n+1} 对应 G 中某个元素 x. 由于我们的新关系，$x=I$；因此，$x^{-1}=I$，$yxy^{-1}=I$，$yx^{-1}y^{-1}=I$，其中 y 是 G 中任何元素. 所以

$$J:\ y_1xy_1^{-1},\ y_1x^{-1}y_1^{-1},\ y_2xy_2^{-1},\ y_2x^{-1}y_2^{-1},\cdots$$

作为关系 $R_{n+1}=I$ 的直接推论是 G 中等于 I 的元素集合. 集合 J 中的这些元素的任何两个的乘积当然也等于 I，这些乘积的乘积也等于 I，等等；也就是说，如 K 是 G 中由 J 中的元素所生成的元素集合，则根据 $R_{n+1}=I$，K 的每个元素都等于 I●. 我们留给读者证明，K 是 G 的子群.

K 是 G 的正规子群吗？K 是正规子群当且仅当

$$yK=Ky \text{ 或 } yKy^{-1}=K,$$

其中 y 是 G 的任意元素. 我们证明对 K 中某特殊元素 k_1 证明 yk_1y^{-1} 是 K 的元素. 我们的方法也可以应用于 K 的任何元素，它根据这样一个事实，即 K 中的任何元素是集合 J 中的元素的字. 假设我们取这特殊的字

$$k_1=(y_1xy_1^{-1})(y_2xy_2^{-1})(y_3xy_3^{-1}),$$

则

$$yk_1y^{-1}=y(y_1xy_1^{-1})(y^{-1}y)(y_2xy_2^{-1})(y^{-1}y)(y_3xy_3^{-1})y^{-1},$$

因为 $y^{-1}y=I$. 所以，由于 $(yy_1)^{-1}=y_1^{-1}y$，我们有

$$\begin{aligned}yk_1y^{-1}&=(yy_1)x(yy_1)^{-1}(yy_2)x(yy_2)^{-1}(yy_3)x(yy_3)^{-1}\\&=\text{集合 } J \text{ 中元素的字}\\&=\text{子群} K \text{ 的元素}.\end{aligned}$$

我们用来证明 yk_1y^{-1} 属于 K 的办法也可用于任何元素 yky^{-1}，其中 k 属于 K. 因此，我们得出结论 yKy^{-1} 的每个元素都属

● 同 68 页上的集合 K 比较一下.

于 K. 并且,这个办法对于 G 中所有元素 y 也对;特别假如 k 是 K 中任何元素,则 $y^{-1}k(y^{-1})^{-1}$ 属于 K. 因此,对于 K 中每个 k, 存在 K 中的元素 $\hat{k}$, 使得

$$\hat{k}=y^{-1}k(y^{-1})^{-1}=y^{-1}ky \quad 或 \quad k=y\hat{k}y^{-1}.$$

这就证明: K 中每个元素都属于集合 yKy^{-1}. 所以 $K=yKy^{-1}$, K 是 G 的正规子群.

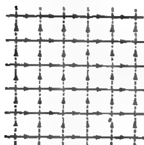


图 11.11

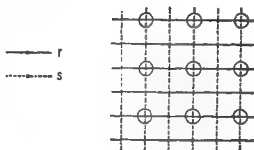


图 11.12

为了说明我们通过添加关系定义商群的一般的命题,我们提出这个例子:

(1) 我们取群 G 为"城市街道"群(81 页),它有生成元 r 及 s, 以及定义关系 $rsr^{-1}s^{-1}=I$ (见图 11.11).

(2) 我们添加关系

$$r^2=I, \quad s^2=I.$$

(3) 由这个新关系以及群的公理直接推出的 G 中等于 I 的元素就是由 r^2 及 s^2 所生成的元素,即所有 G 中形如 $r^{2m}s^{2n}$ 的元素,其中 m 及 n 可取值 0, ±1, ±2, ⋯(即所有 r 及 s 偶数幂生成的字). 这些元素形成正规子群 K. 它们在图 11.12 中表成带○的顶点.(我们省略掉箭头,因为,它们对于表示陪集的分布不太重要.)

(4) 商群 G/K 由扩大关系组

$$r^2 = I, \ s^2 = I, \ rsr^{-1}s^{-1} = I$$

定义. 由前两个关系可推出 $r = r^{-1}$, $s = s^{-1}$, 所以最后一个关系可写作 $rsrs = (rs)^2 = I$. 读者可能已经看出这正是四群的定义关系(76 页).

图11.13 表示商群 G/K 的陪集的分布图.

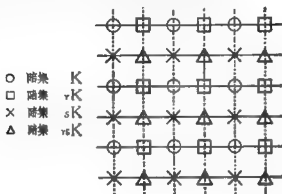


图 11.13

练习 57 假设群 G 具有相伴的商群 G/K. 对于下列诸群的交换性,我们可以推出什么结论?

(a) G/K, 如 G 是交换群, (b) G/K, 如 G 是非交换群,
(c) G, 如 G/K 是交换群, (d) G, 如 G/K 是非交换群.

练习 58 假设 G 有生成元 x 及 y, 具有定义关系 $x^4y^{-3} = I$. 证明 G 是非交换群. [提示: 求出同构于商群 G/K 的熟知的非交换子群再用上面练习的结果.]

第十二章　四　元　数　群

交换群的每一个子群都是正规子群．有没有非阿贝尔群，它的所有子群都是正规子群？有没有非阿贝尔群，它的真子群都不是正规子群？在这两个极端情形下，都有群存在．最小的非阿贝尔群其所有子群是正规子群就是所谓哈密尔顿[1]四元数群，其阶数为 8．而最小的非阿贝尔群它不具有真正规子群的就是阶数为 60 的二十面体群．

二十一面体群在数学发展史上非常有名是因为它在伽罗华研究一般的五次方程的可解性上起着重要作用．伽罗华证明，任何代数方程解的性质依赖于与这方程相关的一个置换群，可解性的关键就在于由其正规子群所得到的商群．对于一般的五次方程，方程的群的有关性质就依赖于二十面体群没有正规子群这个事实．我们将在附录中考察二十面体群．

8 阶四元数群的基本性质是十九世纪四十年代由哈密尔顿发现的．哈密尔顿在物理光学及动力学方面作出重要发现之后，把他的注意力转向探索，如何把复数加以推广，所谓复数就是形如 $a+ib$ 的数(其中 $i=\sqrt{-1}$)．他希望这种广义复数可以用来表示三维空间中的旋转，象通常的复数能用来表示平面的旋转一样．为此目的，哈密尔顿发现必须引进两个新“单位” j 及 k．因为通常的复数是基于两个“单位” 1 及 i 之上，哈密尔顿的推广了的超复数就基于四个“单位” 1，i，j，

---

[1] 威廉·罗文·哈密尔顿 (William Rowan Hamilton 1805—1865)．

k；所以叫作"四元数"．四元数就是这四个单位的线性组合，即形如下式的组合

$$q = \alpha + i\beta + j\gamma + k\delta,$$

其中 $\alpha, \beta, \gamma, \delta$ 是实数．这些新复数的确可以表示三维空间中的旋转(也可以表示四维空间中的旋转)．

根据定义，四元数单位之间满足的基本关系是

$$i^2 = j^2 = k^2 = ijk = -1;$$

由此，我们可以推出

$$ij = k,\ jk = i,\ ki = j.$$

并且

$$ji = -k,\ kj = -i,\ ik = -j.$$

这就表明，四元数单位是非交换的，因而四元数也是非交换的．因为三维空间中的旋转是非交换的．这个结果并不出人意外．

四元数群 Q 的八个元素是

$$1, -1, i, -i, j, -j, k, -k.$$

为了方便起见，让我们令

$$i = a,\ j = b,\ 1 = I;$$

于是 $ab = ij = k$，且群 Q 的定义关系是

$$a^2 = b^2 = (ab)^2.$$

其八个元素是

$$I, a, b, ab, ba, a^2, a^3, b^3.$$

为了得出四元数群的图象，注意下面的式子是有帮助的

$$a^4 = b^4 = (ab)^4 = I.$$

这些关系可以由基本的群的关系导出来．(详见练习 21 的解答．)从关系 $a^4 = b^4 = I$，我们可以想象到群的图中包含两个互相连锁的四边形．四元数群 Q 的图象如图 12.1所示．注意 b 线段彼此跨越但不相交．这个图象实质上是一个嵌入在三

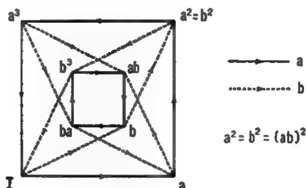


图 12.1

维空间中的网络，把它表示在平面上就在于表出图象的网络的线段的投影的交.

拉格朗日定理告诉我们，Q的任何真子群必是2阶或4阶的.唯一的2阶抽象群(115页)是循环群C_2,而4阶抽象群只有循环群C_4及四群;所以决定出Q中所有元素的周期有助于求出它的子群来. 用Q的图象当作压缩了的乘法表,我们发现a^2是Q中周期为2的唯一的元素,I的周期当然等于1,其他6个元素的周期都是4. 因此我们得出结论，Q包含一个同构于循环群C_2的子群,以及六个同构于C_4的子群.

剩下的问题是,Q中有没有同构于四群的子群呢? 这种可能性必须排除掉,因为我们可以回忆一下,四群中有三个周期为2的不同元素(见76页).

我们断言：非交换群Q的所有子群都是正规子群.首先,我们考察唯一的2阶子群

$$H=\{I, a^2\},$$

决定它是否是正规子群. 我们的方法就是把Q同态映到群Q^*上，使得H映到Q^*的单位元素上. 正如第十一章的例子中我们所采用的办法，我们添加一个关系就等价于把一个子

群映到I上. 我们添加关系$a^2=I$，从而把H映到I上. 这一组扩大的关系

(1) $$I=a^2=b^2=(ab)^2$$

定义某个商群Q^*. H是Q的正规子群当且仅当Q^*是4阶群，也即，当且仅当Q^*的元素是Q关于2阶子群H的陪集. 事实上，我们的确认出这组扩大的关系(1)就是四群的一组定义关系. 因此，H是Q的正规子群. 六个4阶循环群也是正规子群，因为Q的阶数为2×4(见练习52，137页). 因此非阿贝尔群Q的所有子群是正规子群●.

任何非阿贝尔群如其所有子群都是正规子群就称为哈密尔顿群. 四元数群是阶数最小(8阶)的哈密尔顿群. 能够证明，任何有限的哈密尔顿群可以由四元数群及阿贝尔群通过作直积得出来.

● 由这个讨论不能够得出：如果H是G的正规子群，则G中同构于H的任何其他子群也是正规子群. 在第十三章中将要讨论的群S_4有四个子群同构于四群，但其中只有一个是S_4的正规子群.

第十三章　对称群与交代群

现在我们来更仔细地考察一已知有限集合到自身上的所有映射所构成的群．这种群称为对称群．如果已知集合有 n 个元素，其相应的对称群就用 S_n 表示．

假设已知集合只含二个元素，那么组成相应的对称群 S_2 的映射或置换是什么呢？这个群只有两个映射：

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \text{及} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

这两个映射可以几何地解释为一个线段到其自身的重合运动，见图 13.1．这个重合运动群是循环群 C_2，因此 S_2 同构于 C_2．



图　13.1

其次，我们来考虑 S_3．假如我们把一集合 $\{a_1, a_2, a_3\}$ 映到其自身上，对于 a_1 的像我们有三种选法：即 a_1，a_2 或 a_3．当选定任何其中一个之后，我们由剩下的两个元素中选取 a_2 的像．（因为映射是一对一的，所以 a_2 的像只有两种可能．）最后，对于 a_3 的像元素，只有一种可能的选择．因此，三元素集合到自身上的不同映射共有六种，它们是

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}.$$

这些映射可以几何地解释为等边三角形的重合运动（图13.2）。我们认识这个群就是二面体群 D_3。因此，S_3 同构于 D_3

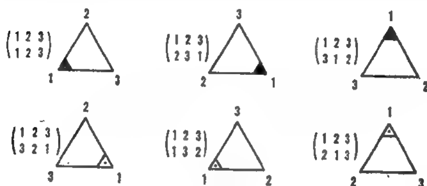


图 13.2

关于 S_4，我们提出下列的命题，但是不给证明也不进一步说明。

（1）一个立方体的所有重合运动的集合是同构于 S_4 的群。

（2）一个正八面体的所有重合运动的集合是同构于 S_4 的群。

（3）这两个多面体群（126 页）都同构于 S_4 这个事实与下面的事实有关：立方体及正八面体是对偶图形。[1]（其他的对偶多面体见附录。）

一般来讲，已知一个集合 $\{a_1, a_2, \cdots, a_n\}$ 把它映到自身

---

[1] 立方体的六个面是正方形，这些正方形的中心构成一个正八面体，即一个有八个面（全等的等边三角形）及六个顶点的多面体。反之，一个正八面体的八个面的中心构成一个立方体的顶点。我们就说这两个多面体互相对偶；某个多面体的重合运动也是另一个多面体的重合运动。一个四面体是自对偶多面体。（见新数学丛书（NML）中第十卷，O. 奥尔（Ore）所著《图及其用途》（Graphs and Their Uses 的 100—106 页。）

上，a_1 的像元素有 n 种选法，a_2 的像有 $n-1$ 种选法，……，最后，a_n 的像元素只有唯一一种可能的选取，因为 $n-1$ 个元素已经被指定为像了．所以，对称群包含有

$$n(n-1)(n-2)\cdots3\cdot2\cdot1$$

种不同的映射或者置换．假如我们引入记号

$$n(n-1)(n-2)\cdots3\cdot2\cdot1=n!,$$

其中 $n!$ 读作“n 的阶乘”，则我们就可以说 S_n 的阶是 $n!$．

对称多项式

对称群与对称多项式密切相关．作为两变量对称多项式的例子，考虑

$$d_2=(x_1-x_2)^2.$$

d_2 的值依赖于 x_1 及 x_2 的值．然而，x_1 与 x_2 对换使得 d_2 的值不改变．在 d_2 中使 x_1 与 x_2 对换实际上意味着，先把集合$\{x_1, x_2\}$ 映到自身上使得 $x_1\to x_2$，$x_2\to x_1$，然后，把 d_2 的多项式表达式中的每个元素换成其像元素．因为 $\{x_1, x_2\}$ 到其自身上的映射只有两个：

$$\begin{pmatrix} x_1 & x_2 \\ x_1 & x_2 \end{pmatrix} \text{及} \begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix},$$

所以，**当把元素替换成对称群 S_2 中任何映射下的像时，d_2 保持不变．**

三变量对称多项式的例子可举

$$d_3=(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2.$$

容易证明：当 x_1，x_2，x_3 替换成对称群 S_3 中的任何映射下的像时，d_3 的值保持不变．

一般来说，n 变量对称多项式是一个多项式，当 n 个变量替换成对称群 S_n 中的任何映射（或置换）的像时，其值保持不变．

对换

如果我们用一种特殊的循环——所谓对换来表示对称群的元素，那么对称群的结构的有趣的特性就变得十分明显。我们在第十章中证明，有限集合到自身上的任何映射可以表示为不同元素的循环的相继；例如

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} = (124)(35).$$

循环 (124) 含有三个不同的记号，而 (35) 只含两个不同的记号．只含两个不同的记号的循环称为对换．我们将证明每个循环可以表示为一串对换．因为对称群中的每个映射均可表为循环的乘积，由此就可推出对称群中的每个元素可表为一串对换．

作为说明，我们断言 $(124) = (12)(14)$． 为验证它，我们回到记号 1, 2, 4 的映射：

(12)		(14)	(12)(14)
$1 \to 2$	跟着	$2 \to 2$，	总结果是 $1 \to 2$，
$2 \to 1$	跟着	$1 \to 4$，	总结果是 $2 \to 4$，
$4 \to 4$	跟着	$4 \to 1$，	总结果是 $4 \to 1$，

因此 (12) (14) 的总结果是 $1 \to 2$, $2 \to 4$, $4 \to 1$，也就是循环 (124)，这就是我们的断言．

任何三个不同记号的循环都可以表示为两个对换相继：

$$(abc) = (ab)(ac).$$

同样，四个记号的循环可以表为三个对换：

$$(abcd) = (ab)(ac)(ad).$$

一般来说，n 个记号的循环可以表为 $(n-1)$ 个对换相继：

$$(a_1a_2\cdots a_n) = (a_1a_2)(a_1a_3)\cdots(a_1a_n).$$

练习 59 证明：假如一个 n 个记号的置换表示为 r 个

循环相继，这 r 个循环有 n 个记号互不重复，则这置换可表为 $n-r$ 个对换相继.

注意：一个映射或置换表示成对换相继的方式并不唯一. 例如，映射

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

可以表示为

$$(123)=(12)(13) \text{ 或 } (231)=(23)(21)$$
$$\text{或 } (312)=(31)(32).$$

我们注意到这些表法中对换的数目都相同. 因此，我们可以猜想：对换的数目是一个映射或置换的特征. 但是，可以举出例子证明对换的数目不是一个置换的固定特征. 考虑

$$(12)(13)(23)=(13).$$

事实上，有无穷多种方式把一个置换表成对换之乘积. 我们只须考虑下列恒等式

$$(ab)(ab)=I \text{ 及 } (ab)=(ca)(cb)(ca).$$

下面我们证明：一个已知置换表示成对换的乘积的无穷多种表法中或者包含偶数个对换，或者包含奇数个对换. 考虑变量 x_1, x_2, x_3 的多项式

$$g_3=(x_1-x_2)(x_1-x_3)(x_2-x_3).$$

(我们只限于讨论三个变量的情形，但是这个推理的方式可马上推广到 n 个变量的情形.) 注意 g_3 是怎么造出来的：它是所有差 $x_j-x_k(j<k)$ 的乘积. 显然，变数的偶数个对换使 g_3 保持不变，而任何奇数个对换使 g_3 变成 $-g_3$. 现在考虑三个变量 x_1, x_2, x_3 的任何置换，或者说，三个指标 1, 2, 3 的任何置换. 这种置换每个都是 S_3 的元素，故可以是对换的相继. 假如，一个特殊的置换 p 使得 g_3 不变，则 p 表示成任何对换

时，必定由偶数个对换构成. 假如 p 把 g_3 变成 $-g_3$，则 p 表示成对换时，必定由奇数个对换构成. 于是，我们得出结论，一个置换不能表示为偶数个对换，同时又能表示为奇数个对换.

一个置换称为偶置换，如果它表为对换的任何一个表示的对换数是偶数，反之称为奇置换. 恒等置换被考虑为偶置换，因为它不包含对换. 一个置换的奇偶性与表成对换的特殊表示法无关.

练习 60 证明 n 个记号的集合的任何置换可表示为只含 $n-1$ 个对换 (a_1a_2)，(a_1a_3)，$\cdots$，(a_1a_n) 的乘积. 由此推出这 $n-1$ 个对换可取为对称群 S_n 的生成元的集合. [提示：利用恒等式 $(ab)=(ca)(cb)(ca)$.]

交代群

特别有趣的是 n 个记号的集合的所有偶置换所成的集合 A_n. 显然，A_n 是 S_n 的一个子群. 为了证明这个命题，我们来验证 A_n 满足子群的两个试验条件.

(1) **封闭性**: 如果 p_1 及 p_2 是 A_n 的置换，它们分别可以表成 n_1 个及 n_2 个对换，则它们的乘积 p_1p_2 可以表成 n_1+n_2 个对换. 如果 n_1 及 n_2 均为偶数，则 n_1+n_2 也是偶数，因此我们得出 p_1p_2 是偶置换，所以属于 A_n 中.

(2) **逆元素**: 如果一置换（在 S_n 中）有逆元素 p^{-1}，则 $pp^{-1}=I$ 只能够表为偶数个对换，因为 I 是偶置换. 因此，如 p 是偶置换，则 p^{-1} 必然也是偶置换；也就是说，A_n 的每个元素在 A_n 中有一个逆元素.

S_n 的子群 A_n 称为交代群. 当我们讨论交代多项式时，这样叫的理由将很快就清楚了.

S_n 的阶是 $n!$（见 155 页）. 我们断言 A_n 的阶是 $1/2n!$，

也就是说，S_n 包含 $1/2\ n!$ 个偶置换及 $1/2\ n!$ 个奇置换.

证明：命 a 为对称群 $S_n(n>1)$ 的任何对换，比如说 $a=(12)=(12)(3)(4)\cdots(n)$. 把 S_n 中的每个元素左边乘上 $a=(12)$. 结果得到的 $n!$ 个元素的集合包含 S_n 中所有元素而没有重复.（根据 39 页定理 1，我们知道这事是对的.）但是，S_n 中的每个偶置换与元素 (12) 的乘积是个奇置换，而奇置换与 (12) 的乘积是个偶置换. 因此，奇置换的集合与偶置换的集合相互之间有一个一对一的映射. 而这只当偶置换与奇置换的数目相等时才有可能. 因此，A_n 的阶为 $1/2n!$，这就是我们的断言.

在练习 52 中已经证明，如果 G 是 $2n$ 阶群，H 是 n 阶子群，则 H 是 G 的正规子群. 因为 A_n 的阶是 $1/2n!$，S_n 的阶是 $n!$，我们得出结论：交代群 A_n 是对称群 S_n 的正规子群. 我们曾经指出，对称群及正规子群在关于代数方程的可解性的伽罗华理论中起着基本的作用. 交代群 A_n 也是该理论的基本组成部分.

A_3 的几何表示

对称群 S_3 同构于二面体群 D_3；见 154 页. 所以 S_3 可以几何地表为等边三角形的对称或重合运动；A_3 是 $1/2\ 3!=3$ 阶子群，包含所有 S_3 的偶置换. 图 13.3 中的第一行三角形的位置对应于偶置换，或者三角形的顶点的偶数个对换. 读者可以把顶点的对换解释为关于某一高线的翻转. 图中第一行的三角形的位置都是经过偶数个翻转得到，第二行的三角形的位置都是经过奇数个翻转得到.

交代多项式

交代群和交代多项式之间有着密切关系. 在我们以前讨

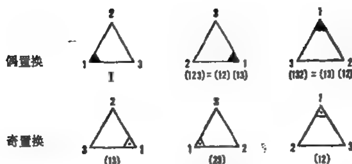


图 13.3

论奇置换及偶置换时，我们引入过交代多项式 g_3。作为两变量交代多项式的例子，考虑

$$g_2 = x_1 - x_2.$$

如把 x_1 与 x_2 互换或者对换奇数次，则 g_2 变成 $-g_2$；但如把 x_1 与 x_2 对换偶数次，则 g_2 不变。两个变量 x_1 与 x_2 的所有置换的集合是对称群 S_2，所以我们可以把关于 $g_2 = x_1 - x_2$ 的观察改述如下：在交代群 A_2 的置换之下，g_2 不变，而 S_2 的奇置换把 g_2 变为 $-g_2$。

这个结果可以推广到 n 个变量的交代多项式 g_n 上，其中

$$\begin{aligned} g_n = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)\cdots(x_1 - x_n) \\ (x_2 - x_3)(x_2 - x_4)\cdots(x_2 - x_n) \\ (x_3 - x_4)\cdots(x_3 - x_n) \\ \cdots(x_{n-1} - x_n). \end{aligned}$$

在交代群 A_n 中的置换之下，多项式 g_n 不变，而 S_n 的奇置换把 g_n 变成 $-g_n$。

我们简单地讨论一下四面体群（见 124 页）A_4 的有趣性质来结束我们这节交代群的讨论。我们所要讨论的主题是关于拉格朗日定理的逆定理。我们在 96 页曾问这样的问题：如果群 G 的阶为 g，如 h 是 g 的因子，那么 G 中是否存在 h 阶的子群呢？A_4 可以用来证明，这个逆定理并不成立。A_4 是 12

阶群，但它没有6阶子群. 因此，拉格朗日定理的逆定理不成立.

但是，g阶群G有h阶子群（其中h是g的因子）的充分条件由下面的西洛❶（Sylow）定理给出:

假设G是g阶群，h是g的因子，如$h=p^n$，其中p是素数，n是正整数，则G有一个h阶子群.

A_4是12阶群，12的素因子是2及3，所以由西洛定理可以推出A_4有阶数为2，2^2及3的子群，但不能推出A_4有6阶子群.

我们列出A_4没有6阶子群的证明步骤的大要，请读者补出证明的细节.

(1) A_4的所有元素(除了I)周期或者为2或者为3.（提示：考虑把A_4的任何元素考虑为循环形式. 见练习62.）

(2) A_4的正规子群中没有周期为3的元素.（提示：证明任何把A_4中周期为3的元素映到I的同态必定把整个群A_4映到I上.）

(3) A_4中的周期为2的元素的集合组成四群（阶数为4）.

(4) 因为A_4的任意真正规子群只包含周期为2的元素，所以这种正规子群的最大可能阶数是4.

(5) A_4没有6阶子群.

练习 61 证明命题(5)；也即证明A_4没有6阶子群.(当然要用到前面四条命题.)

练习 62 考虑记号a，b，c，d的置换的集合. 证明

❶ L. 西洛是挪威数学家，他在1872年发表这个定理. 在这之前，柯西(Cauchy)曾证这个定理的特殊情形$n=1$.

(a) 如果 $x=(abc)$，则 $x^3=I$；(b) 如果 $x=(ab)(cd)$，则 $x^2=I$.

[这个练习与上面命题(1)有关.]

在代数方程的可解性理论中，一个重要的交代群是 A_5，即五个记号的交代群. 这群是二十面体群，它是不具有真正规子群的最小的非阿贝尔群. 读者在附录中可以找到关于群 A_5 及其图象的一些论述.

第十四章　道　路　群

空间中的道路

我们在本章中将讨论道路群，我们的目的是阐明拓扑问题如何自然地得出由生成元及关系表示的群的定义。与道路群相连系的概念的提出很大程度上依赖于读者的空间直觉。

我们来考虑闭道路，其始点及终点都是空间中的某个固定点 P（"原点"）。注意，我们用"道路"而不用"曲线"这词是为了强调我们也要考虑沿着道路的一定的方向。这与我们讨论群的图象中沿定向线段的道路是协调一致的。我们不管道路的形状。相反，我们对改变一条道路的形状的可能后果却感到兴趣。我们把过 P 点的两条道路 a_1 及 a_2 称为"相等"或"相同的道路"，假如我们可以通过连续的变化把 a_1 变形为 a_2。我们已经把这种道路描述为"拓扑等价"（见 55 页）。表示这种相等的另一个词是"同伦"；"相等的"道路 a_1 及 a_2 称为同伦。

乍一看，好象通过 P 的所有闭道路都相等，或同伦。如我们在"空的"空间中取一点 P，则通过 P 的任何闭道路可以连续地缩为点 P。但是，如果我们的空间含有"障碍"，这就不成立了。例如，我们限于讨论平面的情形，假设我们要求道路不许通过平面中已给的某个固定圆盘，则任何闭道路 a_1 能够连续地缩成原点 P，只要道路 a_1 不包围这个固定圆盘。可是，包围这个圆盘的道路 a_2 不能连续地收缩到原点 P 而不通过禁区，同时它也不能变形成 a_1（见图 14.1）。

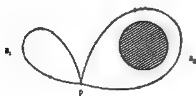


图 14.1



图 14.2

空间中的道路的二元运算

现在我们考虑三维空间中的闭道路，我们定义始于固定点 P 的任意两条闭道路 a_1 及 a_2(图 14.2)的二元运算如下:

(a) 把道路 a_1 的终点从 P 挪开(图 14.3a);

(b) 把道路 a_2 的始点从 P 挪开(图1 4.3b);

(c) 把 a_1 的终点粘到 a_2 的始点上;结果是闭道路 b (图 14.3c).

我们把 b 称为 a_1 及 a_2 的乘积，写作 $a_1a_2 = b$. 不难验证，这个运算是结合的.

我们的目的是造一个群,其元素是同伦道路的集或类,因此,我们需要道路类之间的二元运算.(两个闭道路属于同一类当且仅当它们可以连续地相互变形.)在讨论道路类时，我们用一类中的某一个元素作为整个类的代表. (这个办法类似于我们过去处理同样情况时所采用的办法;例如，16 页,我们用一个旋转代表旋转的集合 A，以及 67 页，我们用一个

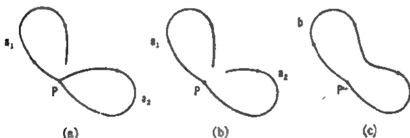


图 14.3

字代表一类等价的字.）于是，我们定义两个同伦道路类的乘积如下：假如 a_1 是第一类的任意道路，a_2 是第二类的任意道路，且 $b = a_1a_2$ 是这两条道路的乘积，则所有同伦于 $b = a_1a_2$ 的所有道路所成的类是两个类的乘积.

我们应该检查一下这个定义的确是确切明白的，也就是说，两类的乘积不依赖于两类中代表的道路的特殊选取. 假设 a_1 及 a_2 是任意两个道路，且 $b = a_1a_2$. 设 a_1^* 为 a_1 同一类中的任意道路（a_1^* 可连续变形成 a_1），a_2^* 为 a_2 同一类中的任意道路，则我们的空间直觉告诉我们：积道路 $b^* = a_1^*a_2^*$ 同伦于道路 $b = a_1a_2$. 因此，两类的乘积不依赖于代表该类的特殊道路 a_1 及 a_2 的选取.

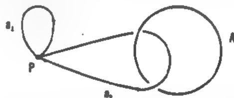


图 14.4

现在，我们在空间中引入"障碍"：假设我们的道路可以穿过三维空间中的所有点，除了一个特殊闭曲线上的点外.（为了确定起见，可以把 A 想象为一个圆周.）如果把 A 想象为由不可穿透的物质构成的，对于我们所讨论的东西的直觉掌握会有帮助.去掉 A 的点后剩下的三维空间的点集称为流形.让我们考察以流形上一点 P 为始点及终点的闭道路，并决定它们的同伦类. 我们只考虑穿过流形的道路，把 A 当作不可穿透的障碍. 至少有两个本质上不同的情况，由图 14.4 中的道路 a_1 及 a_2 所代表（A 的图中的缺口表示道路 a_2 由 A 上面通过，a_2 的图中的缺口表示 a_2 由 A 下面通过）：

(a) 道路 a_1 可由连续变形缩成 P.

(b) 道路 a_2 不能连续变形成 P 而不穿过这不可穿透的障碍.

因此，至少存在两个过 P 点的闭道路的同伦类，一类包含可缩到 P 的道路，表示为 $[I]$；第二类包含可连续变形成 a_2 但是不能缩成 P 的道路，表示为 $[a]$. 类 $[a]$ 中的道路绕 A 一次.

我们已经用记号 $[a]$ 表示同伦于 a_2 的所有道路的集合，也即所有道路具有环绕圆 A 一次的性质，如图所示. 这个集合或类中任意一条道路可以取作整个类的代表. 我们以后用 a 表示这个代表(不必把我们限制于任何特殊的道路上). 一般来说，如果 p 是任何道路，$[p]$ 将表示同伦于 p 的道路类.

道路的逆元素

我们来证明，对于流形中每个同伦道路类，存在一个类 $[b]^{-1}$，$[b]$ 的逆元素，使得 $[b]$ 中任何道路与 $[b]^{-1}$ 中的任何道路的乘积产生出 $[I]$ 中的道路. 换句话说，$[I]$ 可以作为以同伦道路类为元素的群的单位元素.

我们首先描述个别道路的逆元素，然后证明逆元素的类不依赖于代表. 如 b 是通过 P 的任何道路，我们用 b^{-1} 表示道路 b 仅仅改变一下方向. 我们证明，对于任意道路 b，bb^{-1} 及 $b^{-1}b$ 是 $[I]$ 中的道路.



图 14.5

考虑，例如图 14.5 中的道路 a. 我们已经划出一条虚线为其逆元素.（实际上，虚线及实线应该重合但方向相反；我

们把它们稍稍分开一点点为的是能够把每条线都看清楚.)我们用以前描述的方法造乘积 aa^{-1} 及 $a^{-1}a$. 结果得到的道路如图 14.6a 及 14.6b. (同样，其中每一条实际上是由一条由 P 出发的道路和相重的回到 P 的道路构成，但是，我们把这两部分分开.)我们现在看出，不管道路 p 怎么绕出和绕进这个障碍，pp^{-1} 及 $p^{-1}p$ 都能缩成一点. 同样显然，乘积 pp^{-1} (或 $p^{-1}p$) 中的每个因子可以换成任何等价于它的道路；因此，假如 b 同伦于 p，c 同伦于 p^{-1}，bc 可缩成 P，bc 属于 $[I]$. 所以，同伦道路 $[p]$ 的类的逆元素是所有同伦于 p^{-1} 的道路的集合. 于是，如前所定义的，任何类及其逆元素的乘积肯定是类 $[I]$. 我们留给读者证明 $[I]$ 是单位元素，即 $[I][b]=[b][I]=[b]$，其中 $[b]$ 是任何同伦道路类.



图 14.6a



图 14.6b



图 14.7



图 14.8

现在，让我们考察一下由 aa 或 a^2 所代表的道路类. 因为类的乘积 $[a]\cdot[a]$ 不依赖于特殊代表的选取，我们造类 $[a]$ 中两个不同道路的乘积；这些道路在我们的图中 (图 14.7) 记作 a 及 a^*. 我们记得乘积 a^*a 是通过把 a^* 的终点与 a 的始点粘起来而得到的；见 14.8. 我们观察到按照下面的顺序从 A

上面或下面通过(按照箭头的方向)：由 P 开始，从 A 上面通过，从 A 下面通过，从 A 上面通过，从 A 下面通过，回到 P. 因此，道路 a^*a 或 a^2，环绕 A 转二圈. 它可以变形成如图 14.9 所示的道路，显然，它不能变形成类 $[I]$ 的道路或类 $[a]$ 的道路. 道路 a^2 属于一个新的类，我们记作 $[a^2]$ 或 $[a]^2$. 这个类的逆元素 $[a^{-2}]=[a]^{-2}$ 可以用沿着道路 a^2 相反的方向环绕 A 转二圈的道路来代表. 换句话说，道路 a^{-2} 离开 P 后，首先从 A 下面通过，然后从 A 上面通过，然后再从 A 下面通过，最后从 A 上面通过再回到 P.

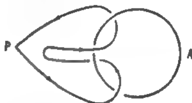


图 14.9

我们用 $[a]^3$ 表示同伦于 $[a^2]$ 中的一条道路与 $[a]$ 中的一条道路的乘积的道路类. 不难看出 $[a]^3$ 中的道路环绕 A 转三次，$[a]^{-3}$ 是沿着相反的方向环绕 A 转三次. 同样，我们可以造出类 $[a]^4$, $[a]^{-4}$, $[a]^5$, $[a]^{-5}$, $\cdots$.

我们的流形中的道路的所有同伦类的集合按下列方式构成群.

群的元素 能够连续互相变形的闭道路的类，这些道路全部在由 A 所决定的流形内，并且全都以 P 为其始点及终点.

结合的二元运算 通过把前面一条代表道路的终点粘到后面一条代表道路的始点，把群的元素相继的连接起来.

单位元素 可以连续变形成 P 的闭道路类 $[I]$.

逆元素 对应于每个道路类，存在唯一的逆元素类，使得

这两类中任何代表元素的乘积属于 $[I]$.

这个群中的元素是

$$\cdots,[a]^{-3},[a]^{-2},[a]^{-1},[I],[a],[a]^2,[a]^3,\cdots.$$

显然,这个群由类 $[a]$ 生成,并同构于无限循环群 C_∞.

由两个圆周所诱导的流形

其次,我们考察由两个互不相交也互不环连的圆周所诱导出的流形中的道路,见图 14.10. 我们的流形现在包含空间中除去两个圆周 A 与 B 以外所有的点. 同前面一样,我们考虑这个流形之内的,以流形中某一固定点 P 为始点及终点的所有闭道路. 只环绕一个圆周的闭道路的类型我们已经讨论过. 我们把只环绕 A 的闭道路类记作 $[a],[a]^2,\cdots$, 把只环绕 B 的闭道路类记作 $[b],[b]^2,\cdots$. 一种新型的道路是既环绕 A 也环绕 B 的道路. 我们来求道路 ab 及 ba, 然后研究这些道路是否可以连续变形成另外一些道路. 这就等价于决定与我们新流形相关的道路群是否可交换.



图 14.10

为了求出道路 ab, 我们把 $[a]$ 中的一条道路 a 的终点粘到 $[b]$ 中的一条道路 b 的始点上;见图 14.11. 注意序列

$$\underbrace{\text{从}A\text{上面,从}A\text{下面}}_{a}\ \underbrace{\text{从}B\text{上面,从}B\text{下面}}_{b}$$

类似,我们可造出道路 ba; 见图 14.12.

我们把逆道路的观念推广到我们的新流形上. 我们把沿

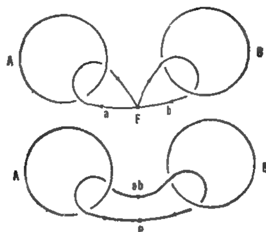


图 14.11

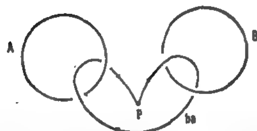


图 14.12

着与箭头方向相反的通过 ba 的道路称为 ba 的逆道路，记作 $(ba)^{-1}$. 我们留给读者去想象

$$(ba)(ba)^{-1} \text{ 及 } (ba)^{-1}(ba)$$

这两条道路都收缩到 P; 它们都在类 $[I]$ 中。 读者还可以由图 14.13 来验证

$$(ba)^{-1} = a^{-1}b^{-1}.$$

现在，我们来考虑可交换性问题： ab 是否与 ba 相等；即道路 ab 能够连续变形成道路 ba 吗？利用我们关于逆道路的知识，我们可以把问题以下面形式重述一下：在我们的流形中，关系

$$(ab)(ba)^{-1} = I \text{ 或 } aba^{-1}b^{-1} = I$$

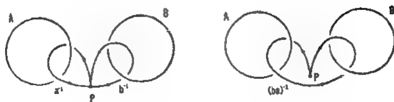


图 14.13



图 14.14

是否成立？

我们通过直接检查道路 $aba^{-1}b^{-1}$ 来回答这个问题．图 14.14 中的道路 $aba^{-1}b^{-1}$ 是把道路 ab 的终点粘在道路 $a^{-1}b^{-1}=(ba)^{-1}$ 的始点上得到的．我们诉诸读者的几何直觉——借助于由一条绳子及两个环所造成的物理模型——使他能够看出这条道路的确可以变形成图 14.15 所示的道路．这种道路称为在由两个互不环连的圆周所诱导出的流形中打

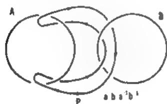




图 14.15　　图 14.16

结．因此，道路 $aba^{-1}b^{-1}$ 不能够收缩成 P，于是我们可以说 $ab\neq ba$．所以与我们的流形相关连的道路群是不可交换的．

有二个环连圆周的新流形

考虑由两个环连的圆周 A 及 B 诱导的流形，见图 14.16. 现在我们不能把一个圆周缩成一点而不穿过另一个圆周.同以前一样，我们的类是除了 A 及 B 以外的空间中所有的点所构成的流形中的道路. 它们仍然是以我们流形中某一固定点 P 为始点及终点的闭道路.

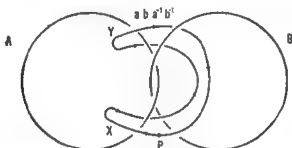


图 14.17

我们造道路 ab 及 ba 决定是否在新流形中 $ab=ba$. 我们用和以前同样的方法造道路 $aba^{-1}b^{-1}$ 并且注意到，在我们这个新的"环连"流形中，同以前"不环连的"流形中的道路一样通过相同的点集(比较图 14.15 及图 14.17). 我们断言,道路 $aba^{-1}b^{-1}$ 能够连续变形使之收缩成点 P; 或者说，道路 $aba^{-1}b^{-1}$ 属于类 $[I]$.

看出道路 $aba^{-1}b^{-1}$ 能够变形成为类 $[I]$ 中的道路的最简易的办法是求助于物理模型. 如果道路 $aba^{-1}b^{-1}$ 具体按照图 14.17 那样作成环(共二个环连的环 A 及 B 的闭线圈),那么可以把线圈从两个环解下来而不撕裂或折断两个环. 为了看出来这点,想象把在 X 处的线圈按照反时针方向沿着 A 滑向 Y，先从圆周 B 上面通过，然后从圆周 B 的下边通过. 这样线圈到达 Y 时,我们看出,这条道路与圆周 B 已不环连. 对于圆周 A 这条道路简单来说是这样: 由 P 开始;在 A 上, 在 A 下;在

A下；在A上。这序列表明，这条道路与圆周A不相环连。因此，这道路 $aba^{-1}b^{-1}$ 属于类 $[I]$，或 $[ab]=[a]\cdot[b]=[b][a]=[ba]$。

由两个环连的圆周诱导出来的流形所对应的道路群的生成元是两条道路 a 及 b（更确切地说道路类 $[a]$ 及 $[b]$）．这两个生成元满足关系 $aba^{-1}b^{-1}=I$．我们以前见过这个群；它是 C_∞^2，“城市街道”群（81 页）。

流形中的打结道路

我们已经看到由两个不环连的圆圈诱导出的流形中，道路 $aba^{-1}b^{-1}$ 是打结的，但是在由两个环连的圆圈所诱导的流形中同样的点集所成的道路却是不打结的．因此，一个特殊闭道路是否打结不仅依赖于道路，而且还依赖于它存在于其内的流形●．

● 图 14.15 及图 14.17 给魔术家的把戏提供一个基础，取两个可以开闭的环（例如，活页笔记本的环），按照图 14.15 的构图用一根线穿过这两个环，最后打上结成一个闭线圈．这个线圈在这两个环上打结．只须把一个环，比如说B打开，然后同环A适当地环连起来，原图形就变成正好是图 14.17 所示的图形．在这个新流形中，闭线圈并不打结，因此能够从环中滑脱出来，这就会使观众目瞪口呆．

第十五章　群与糊墙纸设计

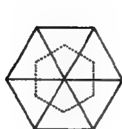
因为群的研究主要涉及结构及关系，所以在"装饰艺术"中出现群的具体显示并不奇怪．事实上，在平面上无限铺开的每种重复的设计总是重复同一个基本图案，就对应一个群．在糊墙纸，纺织品，建筑物装饰等处所用的设计常常属于这种类型，所以，我们无时无刻不在群的表现的包围之中．这种群的表示最终的实现是在格兰那达的阿拉罕布拉宫；摩尔人在十三世纪建成阿拉罕布拉宫之后，在装饰中，把与扩展到整个平面的所有"糊墙纸"群相对应的图案都用上了．

必须注意，存在有二十四个"糊墙纸"群，其中七个的图象只在一个无限带上重复，十七个扩张到整个平面．这些群有时也称作"平面结晶群"，因为结晶体的面上的分子是按照"糊墙纸"类型的重复图案来排列的．

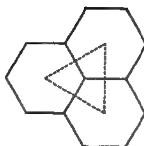
这节中，我们只限于讨论充满整个平面的图案．造出这种图案的一种办法是用全等的正多边形来覆盖平面．可以证明只有三种可能性，如图 15.1 中所画中的（见练习 63）．注意，前两种图案是互相对偶的，也即连结一种图案的中心产生另一种图案的基本要素；第三种是自对偶的．

练习 63　假设平面由正 n 边形所覆盖，使得相邻的 n 边形总是只有一个公共边．证明 n 的值只可能是 3，4，6．

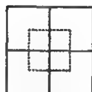
我们对象这些图案的兴趣比起我们对于相应的群的兴趣来说还是第二位的．我们将会看到，图案与运动群相对应，通



三角形



六边形



正方形

图 15.1

过运动群移动基本区域使得它能够覆盖全平面，就好象用某一种基本形状的花砖来铺地面一样.



r 作用后 C 的位置

图 15.2



s 作用后 C 的位置

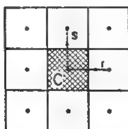
图 15.3

假设我们的基本区域是一个正方形区域 C，考虑两个基本的运动

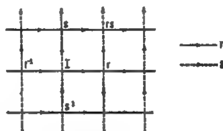
r：把正方形 C 向右平移一边的长度（图 15.2）；

s：把正方形 C 向上平移一边的长度(图 15.3).

我们能用两个生成运动的所有可能的乘积把平面用全等于 C 的区域来覆盖(注意：我们的"乘积"是由相继这二元运算所构成. 因为我们只有一个基本区域，但是要覆盖整个平面，我们可想象 S 在它所占据的每个位置复制自己的象.) 图 15.4a 表明平面上一块区域正在被运动的生成元 r 及 s 逐步覆盖. 这图表示基本区域的中心的象. 注意这些中心的象点对应于



(a) 基本区域 C 及在 r 及 s 下的位移



(b) 具有生成元 r 及 s 及定义关系 $rsr^{-1}s^{-1}=I$ 的群的图

图 15.4

把基本区域覆盖到整个平面的相应运动群的图的顶点(图15.4b). 读者会认出这个群是"城市街道"群 C^2_∞ (81 页).

我们必须明确地区别开这两个图:图 15.4a 基本上是用基本区域 C 的复制品构成的图案画,而图 15.4b 是运动群的图,特别是 C 的平移构成象棋盘的图案. 这两个图之间的相似之点反映出多边形与中心相互变换相应的对偶性. (回忆立方体及八面体,154 页).

除了平移以外我们也能够通过其他运动使基本的正方形在无限的棋盘平面上移动. 这就导出对应于正方形覆盖平面的相同图案的不同的群. 例如,设 a 表示 C 关于其边 c_1 的一个翻转,见图 15.5. 则运动 $aa^2=a^2$ 使 C 回到原来的位置,因此 $a^2=I$. 同样,如果 b 表示 C 关于其边 c_2 的一个翻转(见图 15.6). 图 15.7 表示相继进行运动 a 和 b 的结果. 显然 a 和 b 是不可交换的.



运动 a 后 C 的位置

图 15.5



运动 b 后 C 的位置

图 15.6

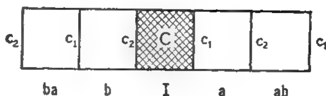


图 15.7

现在假定我们取第三个基本运动为 c：把正方形 C 向上平移一个边的长度. 这三个运动 a, b, c 同两个平移 r 及 s 一样，构成相同的整个棋盘图案，但是，相应的两个群是不一样的. 由 a, b, c 生成的群的图象如图 15.8 所示.



图 15.8

让我们现在开始讨论一种新的基本区域——半正方形或等腰直角三角形——并取生成运动为

r：围绕直角顶点(沿反时针方向)旋转 90°(图 15.9)，

s：围绕弦的中点旋转 180°(图 15.10).

显然 r 的周期为 4，s 的周期为 2.

我们的基本的等腰直角三角形通过运动 r 及 s 产生覆盖平面的图案. 这个图案及相应运动群的图象由图 15.11 表示. 注意后一个图象表示不单用一种，而用两种不同类型的正多边形来覆盖平面的另外一种图样. 在这种图样中，在每个顶点处都有一个正方形与两个正八边形相接.

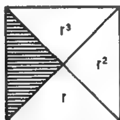


图 15.9



图 15.10

什么是我们所指望的"糊墙纸"的图案呢？它们就是由运动群的图象所展示的图案，而该运动群能够通过一个基本区域来覆盖平面。图 15.11 的图象所展示的糊墙纸图案如图 15.12 所示。

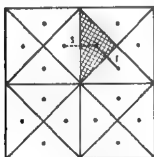
为了得到其他的用不止一种的正多面体来覆盖平面的糊墙纸图案，我们取基本区域为菱形，其中一个角为 60°，取运动的生成元为

r：围绕某个 120° 角的顶点(沿反时针方向)旋转 120°；

s：围绕另外一个 120° 角的顶点（沿反时针方向）旋转 120°。

注意 $r^3 = s^3 = I$；见图 15.13。

图 15.14 表明用菱形覆盖平面，及由 r 及 s 生成的运动群的图象。



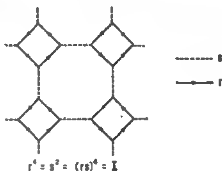
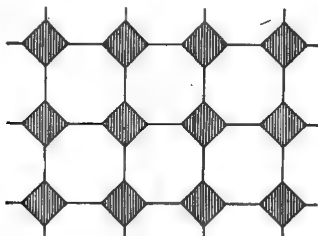


图 15.11



17 种基本不同的糊墙纸图案之一

图 15.12

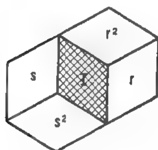
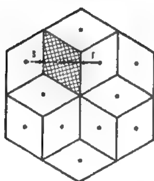


图 15.13



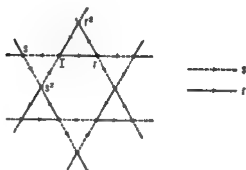


图 15.14

练习 64 求这个群的生成元 r 及 s 的一组定义关系.

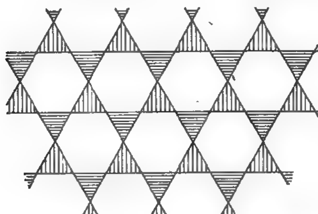


图 15.15

图 15.14 的图表明我们的糊墙纸设计在每个顶点处有两个不同的三角形(一个由 r 线段构成，另一个由 s 线段构成)及两个六边形. 图 15.15 表示这个图案扩展到更大的区域上.

我们现在提供结晶群最后的一个例子. 这一次是在图的每一个顶点处，有三种类型多边形. 我们的基本区域取作角度为 30°, 60°, 90°, 的三角形，运动的生成元是关于三角形

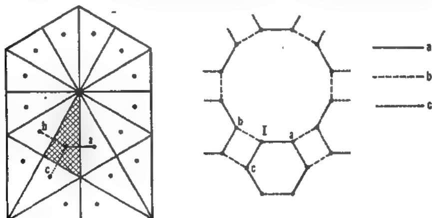


图 15.16

的三个边的翻转. 图 15.16 表明这个图用重复的图案覆盖整个平面，在这个图案中，在每个顶点处，一个正方形，一个正六边形，一个正十二边形相接. 图 15.17 表示这个图在装饰构图中的扩展.

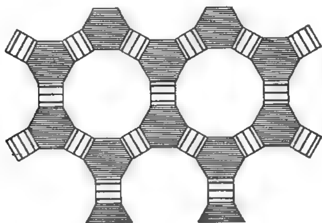


图 15.17

练习 65 求这个群的生成元 a, b, c 的一组定义关系.

附 录

十二面体群及二十面体群：60阶交代群 A_5

相应于十二面体及二十面体的群的结构与我们迄今为止所讨论过的群根本不同．伽罗华在研究代数方程的可解性的过程中，发现正二十面体的重合运动群有许多真子群，但是其中没有任何一个是正规子群．一个没有真正规子群的群称为单群．

十二面体及二十面体有同构的重合运动群因为这两个图形是对偶图形（154 页）：构成十二面体的面的十二个正五边形的"中心"是二十面体的顶点；而构成二十面体的面的二十个等边三角形的中心就是十二面体的顶点．一个图形的叠合运动群与另一个图形的重合运动群完全"相同"．

我们现在数一下二十面体群的元素．假如二十面体的一个顶点固定在"顶上"的位置，则周期为 5 的反时针旋转 72° 就生成所有使"顶上"的顶点不动的所有重合运动；见图 16.1．因为十二个顶点中的每一个都可以送到"顶上"位置，二十面体群的阶为 60．

A_5 的阶是 $\frac{1}{2}5! = 60$（见 158 页），事实上，二十面体群同构于 A_5．下面概要地叙述一下步骤，读者可以按照这种办法证明这个断言是真的．

下面我们描述五个几何对象的集合，这五个几何对象有这个性质：它使二十面体的每个重合运动都导致这五个东西

的一个偶置换一个二十面体有三十条稜及十五条中线——连接一对对边中点的线段．在正二十面体中，这十五条中线组成五个组，每组由三条互相垂直的中线组成，或者说组成五个正交三元组．二十面体的重合运动对应于这五个三元组的偶置换；因为，每一重合运动是下列三种类型之一：

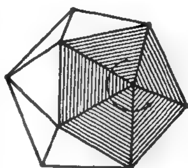


图 16.1

重合运动	偶置换
(1) 围绕连接两个对顶点的对角线的旋转	五个三元组的循环互换，例如 $(abcde)=(ab)(ac)(ad)(ae)$．
(2) 围绕连接两个中心的线段的旋转	五个三元组中的三个循环互换，例如，$(abc)=(ab)(ac)$
(3) 围绕一个中线的旋转	三元组中两对互换，例如 $(ab)(cd)$

类型 (1) 的运动有 24 个，每个周期均为 5；类型 (2) 的运动有 20 个，每个周期均为 3；类型 (3) 的运动有 15 个，每个周期均为 2．

为了求出二十面体群的图，我们首先造一重合运动的图象表示．(见 129 页对四面体群的同样处理．)由此，我们从截断的二十面体出发，也就是把二十面体的每个顶点换成一个对应周期为 5 的旋转 r 的五边形．连接这十二个五边形的顶点的联线对应于一个周期为 2 的翻转，它使进一步旋转中保持不动的顶点更换．把这个构图变形成平面网络，我们可以

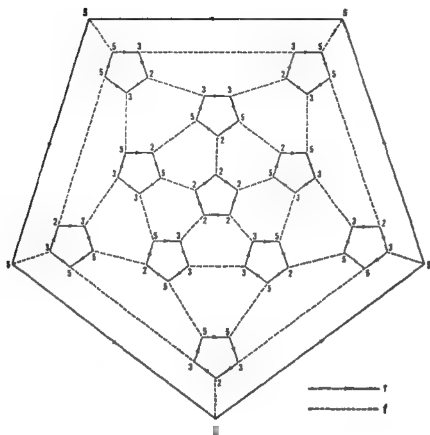


图 16.2

以一个五边形为中心，最后得到图 16.2 的网络。

我们请读者来发掘这个群的内部结构；这图作为一个压缩了的乘法表非常有帮助．为了激起对于这个结构的一些猜想，我们把图 16.2 中的图的每个顶点都标上数目，它表示对应群的元素的周期．(I 已经任意选取．) 我们可以利用 A_5 这个图证明：二十面体群由两个元素 r 及 f 生成，由下面三个关系来定义：

$$r^5 = I,\ f^2 = I,\ (rf)^3 = I.$$

为了证明 A_5 是单群，首先证明，如 g 是 A_5 的任何同态

映射，则 $g(r)=I$ 就蕴涵所有 A_i 都映到 I 上，并且 $g(f)=I$ 也蕴涵所有 A_i 都映到 I 上；然后证明，对于 A 的任何元素 $x \neq I$，$g(x)=I$ 蕴涵 $g(r)=I$ 或者 $g(f)=I$.

习 题 解 答

练习 1 （5 页）：(a) 不是，(b) 是，(c) 不是，(d) 是.

练习 2 （7 页）：$b\otimes c$ 是顺时针转 450°，这相当于将正方形转到重合位置后再转 90°；所以 $b\otimes c=a$. $a\otimes c$ 表示旋转 360°，即转回初始位置.

练习 3 （11 页）：单位元素是 0，这是因为，对于任意实数 x 有 $x+0=0+x=x$.

练习 4 （25 页）：我们立即看到，1 的逆元素是 1；这是因为

$$1\cdot 1\equiv 1 \pmod p.$$

假设 $x\neq 1$，而是

$$2, 3, \cdots, p-1$$

中的一个，考虑 p 个整数 $x, x^2, \cdots, x^p$. 因为 x 和 p 没有公因子，所以这 p 个数都不能被 p 整除. 因此，这 p 个数被 p 除的余数是 $p-1$ 个整数

$$1, 2, \cdots, p-1$$

中的一个，所以至少有两个整数（例如 x^r 和 x^s）有相同的余数，为了确定起见，假设 $0<r<s\leqq p$，则

$$x^s-x^r=x^r(x^{s-r}-1)\equiv 0 \pmod p),$$

且有 $x^r \not\equiv 0$, $x^s \not\equiv 0$ 及 $x^s - x^r > 0$. 由

$$x^r(x^{s-r} - 1) \equiv 0 \text{ 及 } x^r \not\equiv 0$$

我们断定

$$x^{s-r} - 1 \equiv 0 \pmod p.$$

(这里我们利用了如下的事实:以素数 p 为模, $ab \equiv 0 \pmod p$ 当且仅当 $a \equiv 0 \pmod p$ 或 $b \equiv 0 \pmod p$; 读者容易验证这个命题,并用术语"p 的倍数"来解释它).

现在设 y 是 x^{s-r-1} 被 p 除后的余数,则

$$x^{s-r-1} \equiv y \pmod p,$$

两边同乘 x, 得

$$x^{s-r} \equiv xy \pmod p.$$

[验证: 若 $a \equiv b \pmod p$, 则 $xa \equiv xb \pmod p$.] 另一方面,我们已证明 $x^{s-r} - 1 \equiv 0$, 由此推得

$$x^{s-r} \equiv 1 \pmod p,$$

因此 $xy \equiv 1 \pmod p$.

练习 5 (37 页):

(a) 左乘 a^{-1} 得 $bx = a^{-1}c$, 再左乘 b^{-1} 得 $x = b^{-1}a^{-1}c$.

(b) $x = a^{-1}cb^{-1}$, (c) $x = cb^{-1}a^{-1}$,

(d) 在第一个关系式中右乘 x, 则 $ax = bx^3 = bI = b$, 即 $ax = b$, 所以 $x = a^{-1}b$.

(e) $I = x^4 = ax$, 所以 $x = a^{-1}$.

(f) 左乘 x 得 $I = xabc$. 再重复应用右乘,得

$c^{-1} = xab$, $c^{-1}b^{-1} = xa$, $x = c^{-1}b^{-1}a^{-1}$.

练习 6 (42 页): 由乘法表的基本性质(及群的公理)得

(a) $vw = I$, 即 $w^{-1} = v$; $uw = s$, 即 $u = sw^{-1} = sv$;

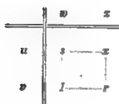
$vz = r$，即 $z = v^{-1}r$；所以 $x = uz = (sv)(v^{-1}r) = sr$.

(b) $uw = I$，即 $u^{-1} = w$；$uz = r$，即 $z = u^{-1}r = wr$；$vw = s$，即 $v = sw^{-1}$；所以

$$x = vz = (sw^{-1})(wr) = sr.$$

(c) $uz = I$，即 $u^{-1} = z$；$uw = s$，即 $w = u^{-1}s = zs$；$vz = r$，即 $v = rz^{-1}$；所以

$$x = vw = (rz^{-1})(zs) = rs.$$



(a)



(b)



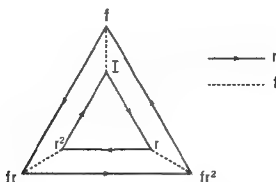
(c)

练习 7 (42 页)：

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

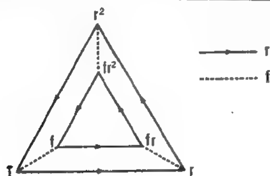
练习 8 (49 页)：(a) 循环群，(b) 循环群，(c) 不是群，因为这个集合不包含加法群的单位元素 0，(d) 循环群.

练习 9 (56 页)：



练习 10 （57 页）：这个乘法表指出做成一个群.（例如，每一个元素都有唯一的逆元素.）注意这个群是可交换的.

	I	r	r^2	f	fr	fr^2
I	I	r	r^2	f	fr	fr^2
r	r	r^2	I	fr	fr^2	f
r^2	r^2	I	r	fr^2	f	fr
f	f	fr	fr^2	I	r	r^2
fr	fr	fr^2	f	r	r^2	I
fr^2	fr^2	f	fr	r^2	I	r



练习 11 (57 页): 字 rsr 对应于如下的道路(它们分别取 A, B, C 作起点):

从 A 到 B 到 C 到 A, 闭的,
从 B 到 C 到 B 到 C, 不闭,
从 C 到 A 到 A 到 B, 不闭.

练习 12 (73 页): 作为由 $frfr^{-2}=I$ 推得的一个结果, 我们有

$$r^2=Ir^2=(frfr^{-2})r^2=frf,$$

由此又推得 $fr^2f=f(frf)f$, 因为 $f^2=I$, $fr^2f=r$, 所以

$$r^2=(fr^2f)(fr^2f)=fr^4f.$$

从而有 $fr^4f=frf$, 这又推得 $r^4=r$ 即 $r^3=I$. 最后有

$$I=r^3=r(r^2)=r(frf),$$

它就是集合中剩下的关系.

练习 13 (74 页): (a) 我们可以写

$$(y^3)^2=(xyx^{-1})(xyx^{-1})=xy(x^{-1}x)yx^{-1}=xy^2x^{-1},$$
$$(y^3)^3=(xy^2x^{-1})(xyx^{-1})=xy^3x^{-1}.$$

用 xyx^{-1} 代替第二个方程中的 y^3, 得

$$x(xyx^{-1})x^{-1}=y^9,\text{ 即 } x^2yx^{-2}=y^9.$$

因为 $x^2=I$ 推得 $x^{-2}=I$, 所以我们能断言 $y=y^9$, 即 $y^8=I$ (y 的周期至多为 8);

(b) 我们有

$$y^{2n}=(y^n)^2=(xyx^{-1})(xyx^{-1})=xy^2x^{-1},$$

类似地有

$$y^{3n}=(y^n)^3=xy^3x^{-1},$$

继续用这种方法我们得到

$$(y^n)^n=y^{n^2}=xy^nx^{-1}=x(xyx^{-1})x^{-1}=x^2yx^{-2}=y$$

(因为 $x^2 = I$)，
因此有

$$y^{n^2} = y, \text{ 即 } y^{n^2-1} = I.$$

所以 y 的周期至多为 $n^2 - 1$。

练习 14 （74 页）：利用练习 13 中的方法得

$$(uvu^{-1})(uvu^{-1}) = (v^4)^2, \text{即} uv^2u^{-1} = (v^4)^2.$$

继续用这个方法我们逐次得到

$$uv^3u^{-1} = (v^4)^3,\ uv^4u^{-1} = (v^4)^4,$$

用 uvu^{-1} 代替 v^4，我们得到

$$u(uvu^{-1})u^{-1} = v^{16}, \text{即} u^2vu^{-2} = v^{16}.$$

因为我们已知 $u^3 = I$，但我们没有关于 u^2 的特殊知识，为了得到 u^3，我们将两边分别乘 v^{16}，得

$$(u^2vu^{-2})(u^2vu^{-2}) = (v^{16})^2, \text{即} u^2v^2u^{-2} = (v^{16})^2,$$

继续下去，逐次得到

$$u^2v^3u^{-2} = (v^{16})^3$$

及

$$u^2v^4u^{-2} = (v^{16})^4,$$

由后者推得

$$u^2(uvu^{-1})u^{-2} = (v^{16})^4, \text{即} u^3vu^{-3} = v^{64}.$$

由 $u^3 = I$ 推得 $v = v^{64}$，即 $v^{63} = I$。所以 v 的周期至多为 63。

(b) 象上面那样，我们得到

$$v^{2k} = (v^k)^2 = (uvu^{-1})(uvu^{-1}) = uv^2u^{-1};$$

$$v^{k^2} = (v^k)^k = uv^ku^{-1} = u(uvu^{-1})u^{-1} = u^2vu^{-2}.$$

从而有

$$(v^{k^2})^k = (u^2vu^{-2})^k = u^2v^ku^{-2} = u^2(uvu^{-1})u^{-2} = u^3vu^{-3},$$

即 $v^{k^3} = u^3vu^{-3}$。继续用这个方法我们得到

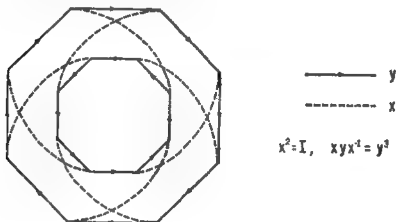
$$v^{k^m} = u^m v u^{-m} = v \text{ (因为 } u^m = I\text{)},$$

所以

$$v^{k^m - 1} = I;$$

v 的周期至多为 $k^m - 1$. (注意，练习 13 及 14 注释了一般的群关系 $(uvu^{-1})^n = uv^n u^{-1}$.)

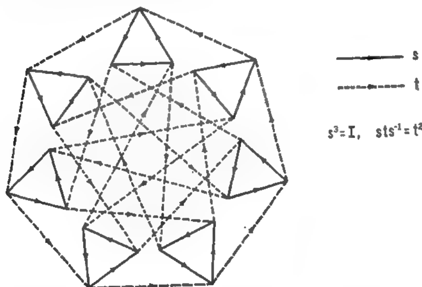
练习 15 (74 页): 由练习 13 我们知道，y 是有限周期的，且 $y^8 = I$. 这就暗示出，其图象的基本图形是八边形. 解法省略，最后得到如下的图象.



练习 16 (74 页): 由练习 14 知道，t 的周期至多为 $k^n - 1$. 设 r 表示 t 的周期(我们假设 $r > 1$，因为否则我们将有特殊情况 $t = I$). 由 $t^r = I$ 推得 $t^{-1} = t^{r-1}$; 类似地，由 $s^n = I$ 推得 $s^{-1} = s^{n-1}$. (这里，我们也假设 $n > 1$，以排除平凡情况，$s = I$). 因此，在任意的字 W 中，我们都可以用 s^{n-1} 代替 s^{-1}，用 t^{r-1} 代替 t^{-1}，所以每个可表示为我们的群的元素的字都能表达成 s 和 t 的正的乘幂项. 现在从给定的关系 $sts^{-1} = t^k$ 着手，右乘 s 得到 $st = t^k s$，所以在任何字中我们都

可用 t^3s 代替 st. 若在一个给定的字中包含序列 st，我们就进行这种替代，我们最后得到的字就是所有 t 的乘幂都在所有 s 的乘幂的左边.因此，我们群中的任意字都是形如 t^xs^y 的字．而且我们可仅选 r 作为 x（因为 $t^r=I$），可仅选 n 作为 y；所以在这个群中至多有 rn 个不同的元素．因为 $r<k^n-1$，所以我们的群至多为 $(k^n-1)n$ 阶.

练习 17 （75 页）：练习 14 告诉我们 $t^7=I$；但因为 7 是素数，所以 t 的周期确为 7．练习 16 使我们推知，我们的群的阶是 21．我们的群的图象可基于 3 个七边形（对应于 $t^7=I$）或 7 个三边形（对应于 $s^3=I$）．这里的（我们的 21 阶群的）图象是基于 7 个三边形.



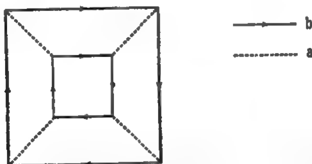
练习 18 （79 页）：我们可利用 $C_2\times C_3$（它有已知关系 $r^3=I$）的图象得到 $g=fr$ 的诸乘幂：

$$g = fr; \qquad g^4 = (fr)^4 = (r^2)^2 = r;$$
$$g^2 = (fr)^2 = r^2; \qquad g^5 = (fr)^5 = (fr)r = fr^2;$$
$$g^3 = gg^2 = (fr)r^2 = f; \quad g^6 = (g^3)^2 = f^2 = I.$$
所以 g 生成循环群 C_6.

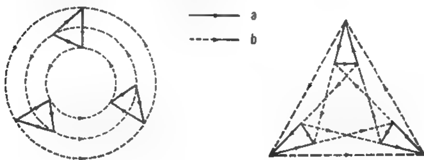
练习 19 (83 页): (a) $C_2 \times C_4$ 由 C_2(生成元 a, 定义关系 $a^2 = I$) 及 C_4(生成元 b, 定义关系 $b^4 = I$) 产生. $C_2 \times C_4$ 的定义要求 a 与 b 是可交换的,即 $ab = ba$, 或 $aba^{-1}b^{-1} = I$. 所以 $C_2 \times C_4$ 有生成元 a 和 b, 有关系

$$a^2 = b^4 = aba^{-1}b^{-1} = I.$$

这些关系对应于 8 阶交换群的图象.



(b) $C_3 \times C_3$ 由生成元为 a 关系为 $a^3 = I$ 的群及生成元为 b 关系为 $b^3 = I$ 的群产生. 因为 a 与 b 在 $C_3 \times C_3$ 中是



可交换的，所以有 $aba^{-1}b^{-1}=I$．因此 $C_3\times C_3$ 是用 a 和 b 生成的并有关系

$$a^3=b^3=aba^{-1}b^{-1}=I.$$

对于这个 9 阶群我们有两个图象(它们拓扑等价吗?)

练习 20 (83 页)：$C_2: a^2=I$．$D_3: r^3=f^2=(rf)^2=I$．因为 a 在 $C_2\times D_3$ 中与 r 及 f 都是可交换的，所以有

$$ara^{-1}r^{-1}=I \text{ 及 } afa^{-1}f^{-1}=I.$$

若有 $C_2\times D_3$ 的元素 x 和 y 使得

$$x^6=y^2=(xy)^2=I \ (D_6\text{的定义关系}),$$

则 D_6 包含 $C_2\times D_3$ 中．因为由 $ar=ra$ 推得 $(ar)^2=a^2r^2=r^2$，且 r^2 的周期是 3，所以 $ar=x$ 的周期是 6．假设取 $y=f$，并看是否有 $(xy)^2=(arf)^2=I$．我们有

$$(arf)^2=a^2(rf)^2=I\cdot I=I.$$

所以元素 $x=ar$ 及 $y=f$ 满足 D_6 的定义关系，从而 D_6 包含在 $C_2\times D_3$ 中．

为了证明 $D_6=C_2\times D_3$，我们仅需指出 $C_2\times D_3$ 与 D_6 有同样多的元素(12 个)．因为 a 与 r 及 f 都是可交换的，所以任何用 3 个生成元排出的字都等价于将其中的 a 的乘幂全移到 r 和 f 的乘幂的左边的字；例如 $farfr^2a^2f=a^3frfr^2f$．所以 $C_2\times D_3$ 中的不同元素的个数是 C_2 中的元素个数 (2) 与 D_3 中的元素个数 (6) 的乘积 $2\times 6=12$．

练习 21 (83 页)：由 $a^2=b^2$ 推得

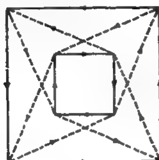
$$a=a^{-1}b^2,\ a=b^2a^{-1} \text{ 及 } ab^{-1}=a^{-1}b.$$

由 $a^2=abab$ 推得

$$a=bab \text{ 及 } ab^{-1}=ba,$$

所以 $a^{-1}b=ba$，因此

$$(ab)^2 = abab = (a^{-1}b^2)b(b^2a^{-1})b = a^{-1}b^5(a^{-1}b)$$
$$= a^{-1}b^5(ba) = a^{-1}(a^6)a = a^6,$$
所以 $a^2 = (ab)^2 = a^6$,由此又推得 $a^4 = I$ 及 $b^4 = I$(因为 $a^2 = b^2$). 所以我们的图象是对应于 $a^4 = b^4 = I$ 的两个互连的四边形. 这是一个 8 阶非交换群的图象,这个群叫做四元数群,第十二章将介绍这个群.



a

b

$a^2 = b^2 = (ab)^2$

练习 22 (83 页):

f

g

(a)

D_∞ 

(b) 设 g 表示元素 rf, 我们可以写

$$f^2 = g^2 = I,\ r = gf^{-1} = gf,\ 及\ r^{-1} = fg.$$

所以用 r 和 f 排的任何字都用 f 和 g 表示.反之,由 $f^2 = g^2 = I$ 推得 $f^2 = (rf)^2 = I$. 因而在用 f 和 g 排的任意字中,我们可用 rf 替代 g 而得到仅用 r 和 f 表示的字.

练习 23 (85 页): 单位元素: 若 a 在 H 中, 则 $aa^{-1} = I$ 在 H 中.

逆元素: 若 b 在 H 中,则 $Ib^{-1} = b^{-1}$ 在 H 中,

封闭性: 若 a 和 b 在 H 中,则 b^{-1} 在 H 中,因而

$$a(b^{-1})^{-1}=ab$$

在H中。

练习 24 (86 页):

(a) 封闭性: $I(ba)=(ba)I=ba$, $(ba)^2=I$.

逆元素: $(ba)^{-1}=ba$, 这是因为 $(ba)^2=I$.

(b) I, a, a^2(它们作成循环群 C_3).

(c) 没有 4 阶子群. 这样的子群应至少包含从两个集合 $\{a, a^2\}$ 和 $\{b, ba, ba^2\}$ 中的每一个来的一个元素，但从这两个集合中的每一个来一个元素作成的对将生成所有 6 个群元素.

练习 25 (87 页): C_5 的元素是

$$a, a^2, a^3, a^4, a^5(=I).$$

a 的周期是 5; C_5 的不是 I 的任意其他元素 a^k 的周期至多是 5,这是因为对 $k=2, 3$或 4 有 $(a^k)^5=(a^5)^k=I$. 若我们假设某个元素 $a^k(1<k<5)$ 的周期是 $n<5$, 则我们引出一个矛盾:

$$(a^k)^n=a^{kn}=I, (\text{这里 } kn \text{ 不是 5 的倍数}).$$

所以 C_5 的(除 I 外的)每一个元素的周期都是 5. 由此推得，C_5 包含的任意子群 $x \neq I$ 应有 5 个不同的元素，因而没有真子群.

练习 26 (88 页):

(a) 封闭性: $3m+3n=3(m+n)$.

逆元素: $3m+(-3m)=0$.

(b) 封闭性: $jn+kn=(j+k)n$,

逆元素: $kn+(-kn)=0$.

练习 27 (88 页): 用 $R \cap S$ 表示R和S的所有公共元素的集合.

封闭性: 设 t_1 和 t_2 在 $R \cap S$ 中,这意味着 t_1 和 t_2 在 R 中,且 t_1 和 t_2 也在 S 中. 因为 R 和 S 是群,所以 t_1t_2 在 R 中也在 S 中,因而在 $R \cap S$ 中.

逆元素: 若 t 在 $R \cap S$ 中, 则 t 因而 t^{-1} 在群 R 中; t 因而 t^{-1} 也在 S 中. 所以 t^{-1} 在 $R \cap S$ 中.

练习 28 (88 页): (a) 因为

$$(a + ib) + (x + iy) = (a + x) + i(b + y)$$

及

若 a, b, x, y 是整数,则 $a + x$ 和 $b + y$ 也是整数,所以加法在我们的集合上是结合的二元运算.

单位元素: $(a + ib) + 0 = a + ib = 0 + (a + ib)$.

逆元素: $(a + ib) + (-a - ib) = 0$.

(b) 封闭性: $(r + is) + (x + iy) = (r + x) + i(s + y)$, 而且若 r, s, x, y 是偶数, 则 $r + x$ 及 $s + y$ 也是偶数.

逆元素: $(r + is) + (-r - is) = 0$.

练习 29 (92 页): 假设陪集 rH 和 sH 至少有一个元素是公共的, 例如 $rh_1 = sh_2$, 则 $s^{-1}r = h_2h_1^{-1}$ 是H的一个元素, 而且 $s^{-1}rh = h_2h_1^{-1}h$ 将表示H的所有元素(当 h 顺次表示H的每一个元素时). 因而 $s(s^{-1}rh) = s(h_2h_1^{-1}h)$, 即 $rh = s(h_2h_1^{-1}h)$, 因而 $rH = sH$. 所以只要这两个陪集有一个公共元素,它们就是恒等的.

练习 30 (95 页): (a) 陪集 $rJ = \{rj_1, rj_2, \cdots\}$. 设 c

是这个陪集 rJ 的一个元素：$c = rj_k$，则陪集

$$cJ = (rj_k)J = \{r(j_kj_1), r(j_kj_2), \cdots\}.$$

但元素 $j_kj_1, j_kj_2, \cdots$ 仅是群 J 的元素的一种重新排列，所以有 $cJ = rJ$.

(b) 若 $r^{-1}c$ 在 J 中，则我们可以写

$$r^{-1}c = j_k,\ (j_k \text{ 是 } J \text{ 的一个元素}).$$

左乘 r 得 $c = rj_k$，这说明 c 在 rJ 中，因而

$$\text{陪集 } cJ = \text{陪集 } rJ.$$

其次假设陪集 cJ = 陪集 rJ，则 cJ 中的任意一元素 cj_k 等于 rJ 中的某个元素 rj_n，即

$$cj_k = rj_n\ (\text{其中 } j_k \text{ 与 } j_n \text{ 都是 } J \text{ 的元素}),$$

左乘 r^{-1} 得

$$r^{-1}cj_k = j_n,$$

再右乘 j_k^{-1} 得

$$r^{-1}c = j_nj_k^{-1}.$$

因为 j_k 和 j_n 在子群 J 中，所以 j_k^{-1} 及 $j_nj_k^{-1} = r^{-1}c$ 也在 J 中.

练习 31 (95 页)：证明可基于这样的观念：若 xJ 和 yJ 是 L 的两个不同的左陪集，则 Jx^{-1} 和 Jy^{-1} 是两个不同的右陪集. 或者反过来说，若 Jx^{-1} 和 Jy^{-1} 不是不同的，则 xJ 和 yJ 也不是不同的. 为了看出这一点为真，我们假设 Jx^{-1} 的一个元素与 Jy^{-1} 的某个元素相等，例如，$j_1x^{-1} = j_2y^{-1}$，则

$$x^{-1} = j_1^{-1}j_2y^{-1} \text{ 因而 } x = yj_2^{-1}j_1 = y(j_2^{-1}j_1)$$

是 yJ 的一个元素. 所以若 Jx^{-1} 和 Jy^{-1} 不是不同的，则 xJ 和 yJ 有公共元素 x，因而也不是不同的. 因为所有左陪集是不同的是已知的，所以所给定的右陪集也是不同的.

练习 32 (95 页)：

左陪集：$K=\{I, a, a^2\}$ 和 $bK=\{b, ba, ba^2\}$，

右陪集：$K=\{I, a, a^2\}$ 和 $Kb=\{b, ab, a^2b\}$。

因为 $(ba)^2=baba=I$，所以我们看到

$$ba=a^{-1}b^{-1}=a^2b.$$

类似地有 $ab=ba^2$。所以左陪集和右陪集是相等的。

练习 33 （96 页）：(a)封闭性：对H的任意两个元素都有 $a^ja^k=a^{j+k}$。因为

$j+k=nq+r$（这里 q 和 r 是整数，且 $0\leqslant r<n$），

所以

$$a^{j+k}=(a^n)^qa^r=a^r$$

是H的一个元素；

(b) 若 g 是G的阶，n 是G的一个元素的周期，则 g 是 n 的倍数(由拉格朗日定理知)。换句话说，有限群的任意元素的周期是这个群的阶的因子。

练习 34 （96 页）：(a) 因为 g 的周期是 n，而 1 是这个"剩余"群的单位元素，所以我们有

$$g^n\equiv 1 \pmod p\text{，即 } g^n-1\equiv 0 \pmod p.$$

(b) 因为 n 是 g 的周期，所以（由练习 33 的 (b) 知）$p-1$ 必是 n 的倍数，即 $p-1=kn$。又因为 $g^n\equiv 1 \pmod p$，所以必有

$$(g^n)^k\equiv 1 \pmod p,$$

即

$$g^{p-1}-1\equiv 0 \pmod p,$$

这也就是说，$g^{p-1}-1$ 是 p 的倍数。

练习 35 （97 页）：因为 a 不是 p 的倍数，所以有 $a\not\equiv 0$

$(\mathrm{mod}\ p)$;由此推得

$$a \equiv r(\mathrm{mod}\ p), (r \text{ 是 } 1, 2, \cdots, p-1 \text{ 中的一个}).$$

所以 $a - r \equiv 0(\mathrm{mod}\ p)$. 现在考虑

$$a^{p-1} - r^{p-1} = (a - r)(a^{p-2} + a^{p-3}r + \cdots + r^{p-2}).$$

因为 $a - r \equiv 0(\mathrm{mod}\ p)$, 所以我们有

$$a^{p-1} - r^{p-1} \equiv 0 \ (\mathrm{mod}\ p),$$

(注意,模一个素数时, $ab \equiv 0$ 当且仅当 $a \equiv 0$ 或 $b \equiv 0$), 即

$$(a^{p-1} - 1) - (r^{p-1} - 1) \equiv 0 \ (\mathrm{mod}\ p),$$

由练习 34 的 (b) 知, $r^{p-1} - 1 \equiv 0 \ (\mathrm{mod}\ p)$, 所以我们有 $a^{p-1} - 1 \equiv 0(\mathrm{mod}\ p)$, 因而

$$a^p - a = a(a^{p-1} - 1) \equiv 0 \ (\mathrm{mod}\ p),$$

这就证明了费马小定理.

练习 36 (97 页): (a) 设 x 是 ab 的周期, y 是 ba 的周期;我们可以写

$$(ab)^x = a(ab)^{x-1}b = I,$$

左乘 a^{-1} 后再右乘 b^{-1}, 得

$$(ab)^{x-1} = a^{-1}b^{-1} = (ba)^{-1};$$

另一方面,

$$(ba)^{x-1} = (ba)^x(ba)^{-1};$$

由此推得 $(ba)^x = I$. 因为 y 是 ba 的周期,所以 x 是 y 的正倍数. 对 $(ba)^y$ 应用相同的方法得知 y 是 x 的正倍数. 所以 $x = y$.

(b) 设 m 是 a 的周期, n 是 b 的周期. 我们需要证明的是 $(ab)^{mn} = I$, 因为由此推得 mn 是 ab 的周期. 因为 $ab = ba$, 所以我们能自由地改变 a 与 b 在乘积 $(ab)^k$ 中的次序. 因此有

$$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n \cdot (b^n)^m = I \cdot I = I.$$

(c) 假设 ab 的周期是 r. 由 (b) 知道, r 是 mn 的因子, 因此 r 必须是 m_1n_1 形的,其中 m_1 是m的因子, n_1 是 n 的因子(包含 $m_1=1$ 或 $m_1=m$ 的可能性). 于是

$$I=(ab)^r=(ab)^{r(m/m_1)}=(ab)^{m(r/m_1)}=(ab)^{mn_1}$$
$$=a^{mn_1}\cdot b^{mn_1}=b^{mn_1} \text{ (因为 } a^m=I\text{)}.$$

由 $b^{mn_1}=I$ 推得 mn_1 是 n 的倍数, 例如 $mn_1=kn$. 由此得 $m=k(n/n_1)$, 所以m的所有的素因子必在整数k和n/n_1的素因子中. 但由于m与n是互素的,所以m与n/n_1也是互素的, 因此m的素因子分解恰好就是k的素因子分解. 所以 $n/n_1=1$ 或 $n=n_1$; 类似地,由

$$I=(ab)^{r(n/n_1)}=a^{m_1n}$$

推得 $m=m_1$. 所以 $r=m_1n_1=mn$.

练习 37 (110 页): 我们证明逆命题: 若映射 f 是同态,则 $f(I)=I$. 对G的任意元素 r 有

$$f(r)=f(Ir)=f(I)f(r).$$

右乘 $[f(r)]^{-1}$ 得 $I=f(I)$ (在H中).

练习 38 (110 页): 我们有

$$I=f(I)=f(xx^{-1})=f(x)f(x^{-1}),$$

即 $I=f(x)f(x^{-1})$, 左乘 $[f(x)]^{-1}$ 得

$$[f(x)]^{-1}=f(x^{-1}).$$

练习 39 (111 页):

$$\begin{aligned} f(xy^{-1}) &= f(x)f(y^{-1})=f(x)[f(y)]^{-1} && \text{(由练习 38 知)}\\ &= f(y)[f(y)]^{-1} && \text{(因为 } f(x)=f(y)\text{)}\\ &= I; \end{aligned}$$

类似地有 $f(x^{-1}y)=I$.

练习 40 (111 页): (a) $f(xy)=f(x)f(y)=I\cdot I=I$.

(b) 由假设有 $f(xy)=f(x)f(y)$,因而 $f(y)=[f(x)]^{-1}$,所以

$$f(yx)=f(y)f(x)=[f(x)]^{-1}f(x)=I.$$

练习 41 (116 页): 我们将证明,将 G 中的每个整数 n 映到 $2n$ 上的映射 f 具有所有所需的性质. 在映射 $f(n)=2n$ (即 $n\to 2n$) 下,有

$$f(m+n)=2(m+n)=2m+2n=f(m)+f(n).$$

而且 $f(m)=f(n)$ [意即 $2m=2n$]是真的,当且仅当 $m=n$. (能有一个同构映射将一个有限群映到它的真子群上吗?)

练习 42 (116 页): 能用

$$r^k\ (k=0,\pm 1,\pm 2,\cdots)$$

表示G的任意元素,H的任意元素为

$$r^{kn}\ (k=0,\pm 1,\pm 2,\cdots).$$

若 x 是G的任意元素,设 f 是映射

$$f(x)=x^n\ (\text{即 } x\to x^n),$$

则对G的任意两个元素 x 和 y 有

$$\begin{array}{ll} G & H \\ x\to x^n & \\ y\to y^n & \\ xy\to (xy)^n=x^ny^n & (\text{因}G\text{是交换群}), \end{array}$$

即 $f(xy)=f(x)f(y)$. 因此,映射 f 是G到H上的一个同态. 其次我们证明

$$f(x)=f(y)\ \text{推得}\ x=y.$$

因为 x 和 y 是G的元素,所以它们的形状为 r^k:

$$x=r^a,\ y=r^b,$$

所以

$$x^n = r^{an}, \quad y^n = r^{bn}.$$

因此

$$f(x) = f(y) \text{ 当且仅当 } r^{an} = r^{bn},$$

在无限循环群中，它成立的充要条件是

$$an = bn, \text{ 即 } a = b.$$

所以 $x = y$，从而 f 是一个同构.

练习 43 (116 页)：若 x 是 G 的任意元素，它能表示成

$$r^k \ (k = 0, \pm 1, \pm 2, \cdots).$$

用

$$r^k \to I \text{ (若 } k \text{ 是偶数)}, \quad r^k \to b \text{ (若 } k \text{ 是奇数)}$$

定义 $f: G \to H$. 若 $x = r^{k_1}$ 和 $y = r^{k_2}$，则

$$xy = r^{k_1} r^{k_2} = r^{k_1+k_2} \begin{cases} \to I \text{ (若 } k_1 + k_2 \text{ 是偶数)}, \\ \to b \text{ (若 } k_1 + k_2 \text{ 是奇数)}. \end{cases}$$

$k_1 + k_2$ 是偶数，当且仅当 k_1 和 k_2 都是偶数或都是奇数，即不是

$$f(x) = f(y) = I$$

就是

$$f(x) = f(y) = b.$$

在这两种情况中都有

$$f(xy) = f(x)f(y) = I.$$

若 k_1 或 k_2 仅有一个是奇数，另一个是偶数，则

$$f(xy) = b \text{ 及 } f(x)f(y) = bI = b,$$

所以也有 $f(xy) = f(x)f(y)$. 因此映射 f 是同态. 因为无限集合 G 到有限集合 H 上的任意映射都不可能是一一的，所以它不可能是同构.

练习 44 （116 页）：若 x 和 y 是 G 的任意两个元素，映射 f 是

$$x \to r^{-1}xr$$

$$y \to r^{-1}yr$$

$$xy \to r^{-1}(xy)r = r^{-1}x(rr^{-1})yr = (r^{-1}xr)(r^{-1}yr)$$

$$f(xy) = f(x)f(y).$$

所以 f 是同态映射. 为了验证同构，我们看到

$$f(x) = r^{-1}xr = r^{-1}yr = f(y) \text{ 当且仅当 } x = y,$$

所以 f 是同构映射.

练习 45 （116 页）：f 是同态的必要条件是 G 是交换群. 为了看出这一点，我们只须指出：由

$$f(xy) = (xy)^2,\ f(x)f(y) = x^2y^2,\ (xy)^2 = x^2y^2,$$

能推得 $yx = xy$. 然而 G 是交换群不是充分条件，它不能确保映射 $f(x) = x^2$ 是一个同构. 这是因为，例如在交换群 C_2 中，因为对所有的元素 x 都有 $x^2 = I$，C_2 又只有两个元素 I 及 b，所以 f 将 C_2 的每一个元素都映到单位元素上. 更一般地说，若 G 有一个偶数周期的元素 $x(\neq I)$，则 $f(x) = x^2$ 不是同构；这是因为，若 $2n$ 是元素 x 的周期，则两个不同的元素 I 和 $x^n(\neq I)$ 都映到 I 上：

$$I \to I^2 = I \text{ 及 } x^n \to (x^n)^2 = x^{2n} = I.$$

实际上，确保 $f(x) = x^2$ 是同构的充分条件是：*G是交换群而且G不含有偶数周期的元素*. 因为，若 $x \neq y$，则在 G 中有一个元素 $r = xy^{-1}$ $(r \neq I)$，使得 $x = ry$，所以 $x^2 = xry$. 现在假设 $x^2 = y^2$，则 $xry = y^2$，从而 $xr = y$，所以 $r = x^{-1}y = (xy^{-1})^{-1} = r^{-1}$；但如果 $r = r^{-1}$，则 $r^2 = I$，这与 G 没有偶数周期的元素的假设矛盾. 所以假设 $x \neq y$ 及 $x^2 = y^2$ 将推得一个矛盾，从而映射 $x \to x^2$ 是一个同构. （实际上，没有偶数

周期的元素的有限群和无限群是有的，这意味着，不是每个元素 $x(\neq I)$ 的周期为奇数，就是对所有的 n 都有 $x^n \neq I$。）

练习 46 （122 页）：(a) 我们想证明 $(1234)^2=(13)\cdot(24)$。(1234)(1234) 按如下方式映射 1 和 3：

$$1\to 2,\ 2\to 3\ (\text{即 } 1\to 3),$$
$$3\to 4,\ 4\to 1\ (\text{即 } 3\to 1).$$

所以我们有一个闭循环 (13)；2 和 4 的映射是

$$2\to 3,\ 3\to 4\ (\text{即 } 2\to 4),$$
$$4\to 1,\ 1\to 2\ (\text{即 } 4\to 2),$$

所以 $(1234)^2=(13)(24)$。

(b) (13)(24)(13)(24)：$1\to 3$，$3\to 1$（即 $1\to 1$）；$2\to 4$，$4\to 2$（即 $2\to 2$）。类似地有 $3\to 3$ 及 $4\to 4$。所以 $m_3^2=I$。

(c) $m_2^3=m_2^2m_2=m_3m_2=(13)(24)(1234)$：

$$1\to 3,\ 3\to 4\ (\text{即 } 1\to 4),$$
$$4\to 2,\ 2\to 3\ (\text{即 } 4\to 3),$$
$$3\to 1,\ 1\to 2\ (\text{即 } 3\to 2),$$
$$2\to 4,\ 4\to 1\ (\text{即 } 2\to 1).$$

所以总的结果是 $(1432)=m_4$。

(d) (1234)(1432)：

$$1\to 2,\ 2\to 1\ (\text{即 } 1\to 1),$$

类似地有

$$2\to 2,\ 3\to 3 \text{ 及 } 4\to 4,$$

所以总的结果是 $m_2m_4=I$。

这些关系使我们可以构造元素为 m_1，m_2，m_3 及 m_4 的群 M 的乘法表。

练习 47 (122 页):

$$\begin{pmatrix} m_1 & m_2 & m_3 & m_4 \\ I & a & a^2 & a^3 \end{pmatrix}$$

练习 48 (123 页): (a) $m_2^2 = (12)(34)(12)(34) = I$,

$$m_3^2 = (13)(24)(13)(24) = I,$$

$$(m_2m_3)^2 = (12)(34)(13)(24)(12)(34)(13)(24) = I.$$

(b) 因为 $m_2m_3 = (12)(34)(13)(24) = (14)(23) = m_4$, 所以同构映射是

$$\begin{pmatrix} m_1 & m_2 & m_3 & m_4 \\ I & a & b & ab \end{pmatrix}.$$

练习 49 (125 页):

	I	r	r^2	f	rf	fr	
	g_1	g_2	g_3	g_4	g_5	g_6	
I	g_1	g_2	g_3	g_4	g_5	g_6	$\begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{pmatrix} = g_1$
r	g_2	g_3	g_1	g_5	g_6	g_4	$\begin{pmatrix}1&2&3&4&5&6\\2&3&1&5&6&4\end{pmatrix} = (1\,2\,3)(4\,5\,6) = g_2$
r^2	g_3	g_1	g_2	g_6	g_4	g_5	$\begin{pmatrix}1&2&3&4&5&6\\3&1&2&6&4&5\end{pmatrix} = (1\,3\,2)(4\,6\,5) = g_3$
f	g_4	g_6	g_5	g_1	g_3	g_2	$\begin{pmatrix}1&2&3&4&5&6\\4&6&5&1&3&2\end{pmatrix} = (1\,4)(2\,6)(3\,5) = g_4$
rf	g_5	g_4	g_6	g_2	g_1	g_3	$\begin{pmatrix}1&2&3&4&5&6\\5&4&6&2&1&3\end{pmatrix} = (1\,5)(2\,4)(3\,6) = g_5$
fr	g_6	g_5	g_4	g_3	g_2	g_1	$\begin{pmatrix}1&2&3&4&5&6\\6&5&4&3&2&1\end{pmatrix} = (1\,6)(2\,5)(3\,4) = g_6$

练习 50 （126 页）：我们证明，给定的循环满足（有生成元 $a=(123)$ 及 $c=(12)$ 的）D_3 的定义关系 $a^3=c^2=(ac)^2=I$.

$$a^2=(123)(123)=(132)=b;$$
$$ac=(123)(12)=(1)(23)=(23)=e;$$
$$a^3=a^2a=(132)(123)=(1)(2)(3)=I;$$
$$ca=(12)(123)=(13)(2)=(13)=d.$$

所以，$a=a$, $a^2=b$, $a^3=I$, $c=c$, $ac=e$, $ca=d$; 从而 $a^3=I$, $c^2=I$, $(ac)^2=I$.

练习 51 （130 页）：
$$\begin{aligned} rfr^2\cdot r^2fr &= rf(r^3)rfr \\ &= rfrfr \quad (\text{因 } r^3=I) \\ &= rfrfr(f^2).(\text{因 } f^2=I) \\ &= (rfrfrf)f \\ &= f. \quad (\text{因}(rf)^3=I). \end{aligned}$$

练习 52 （137 页）：若 a 是 G 的任意元素，但不在 H 中，则因 G 的阶是 $2n$, H 的阶是 n, 所以关于 H 的左陪集是 H 和 aH, 而关于 H 的右陪集是 H 和 Ha. 显然 aH 和 Ha 表示用 n 个在 G 中但不在 H 中的元素组成的同一集合，即 $aH=Ha$, 所以 H 是一个正规子群.

练习 53 （137 页）：根据定理 1（39 页）我们知道，xg_1, xg_2, $\cdots$ 是 G 的所有元素，（根据同一个定理）所以 $(xg_1)x^{-1}$, $(xg_2)x^{-1}$, $\cdots$ 是 G 的所有元素.

练习 54 （137 页）：若 $x=yxy^{-1}$, 则右乘 y 得 $xy=yx$; 反之，若 x 与 y 是可交换的，则 $x=yxy^{-1}$. 所以，x 关于 y 是自共轭的，当且仅当 x 与 y 可交换.（若 x 关于 y 是自共轭

的，则 $x(yx^{-1})=yxy^{-1}(yx^{-1})=y$，所以 y 关于 x 是自共轭的.）

练习 55 （137 页）：因为 K 是 G 的正规子群，所以对 G 的任意元素 g 有 $gK=Kg$，即 $\{gk_1, gk_2, \cdots\}$ 与 $\{k_1g, k_2g, \cdots\}$ 包含相同的元素．由此推得，用 g^{-1} 右乘 gK 的每一个元素得到的集合恰好是用 g^{-1} 右乘 Kg 的每一个元素得到的集 K．反之，假设 G 的子群 K 有如下性质：对 G 中的任意 g，$gKg^{-1}=K$，则容易看到 $gK=Kg$，即 K 是 G 的正规子群.

练习 56 （140 页）：(a)(1) 首先假设 $R\cdot S=S\cdot R$，由此来推导 $R\cdot S$ 是一个子群.

封闭性：考虑集合 $R\cdot S$ 的任意两个元素（例如 r_1s_1 及 r_2s_2）的乘积：

$$(r_1s_1)(r_2s_2)=r_1(s_1r_2)s_2.$$

因为 $R\cdot S=S\cdot R$，所以集合 $S\cdot R$ 的元素 r_1s_2 等于 $R\cdot S$ 的某个元素，例如说 $r_1s_2=r_3s_3$；所以

$$(r_1s_1)(r_2s_2)=r_1(r_3s_3)s_2=(r_1r_3)(s_3s_2)$$

是 $R\cdot S$ 的一个元素.

逆元素：将 r_1s_1 作为 $R\cdot S$ 的代表元考虑，显然它的逆元素 $(r_1s_1)^{-1}=s_1^{-1}r_1^{-1}$ 是 $S\cdot R$ 的一个元素，按假设有 $R\cdot S=S\cdot R$，所以 $(r_1s_1)^{-1}$ 也在 $R\cdot S$ 中.

(2) 我们现在假设 $R\cdot S$ 是一个子群，来推导 $R\cdot S=S\cdot R$．为此用 r_1s_1 表示 $R\cdot S$ 的任意元素，用 s_2r_2 表示 $S\cdot R$ 的任意元素，我们将证明 r_1s_1 在 $S\cdot R$ 中而 s_2r_2 在 $R\cdot S$ 中．我们注意 $(r_1s_1)^{-1}$ 在子群 $R\cdot S$ 中，所以

$$(r_1s_1)^{-1}=R\cdot S \text{ 的某个元素 }=r_js_k$$

因而

$$r_1s_1 = (r_js_k)^{-1} = s_k^{-1}r_j^{-1}$$

是 $S \cdot R$ 的一个元素，并且因为 $R \cdot S$ 是一个子群，所以

$$s_2r_2 = (r_2^{-1}s_2^{-1})^{-1}$$

在 $R \cdot S$ 中．所以 $R \cdot S = S \cdot R$．

(b) 现在我们假设 R 是一个正规子群，我们想要证明的是 $R \cdot S = S \cdot R$ 是一个子群．为此设 s 是 S 的任意元素，由 R 的正规性有 $sR = Rs$（对 S 中的每一个 s）．因为 $S \cdot R$ 恰好是所有的集合 sR 的并集（这里 s 在 S 中），而且 $R \cdot S$ 是集合 Rs 的并集，由此推得 $R \cdot S = S \cdot R$．由 (a) 推得 $R \cdot S = S \cdot R$ 是一个群．

练习 57 （148 页）： G 是可交换的当且仅当，任意两个生成元 r_i 及 r_j 满足关系

$$r_ir_jr_i^{-1}r_j^{-1} = I \text{（或 } r_ir_j = r_jr_i\text{）}. \qquad (1)$$

若 (1) 对 G 的生成元是真的，则对 G/K 的生成元当然为真，因为 G 的任意关系都是 G/K 的关系；但反之则不必为真．

(a) 若 G 是可交换的，则 (1) 在 G 中成立因而在 G/K 中也成立．所以 G/K 也是可交换的．

(b) 若 G 是可交换的，(1) 在 G 中不真．仅当 (1) 是附加关系推得的一个结果时，G/K 才是可交换的；否则不是可交换的．

(c) 若 G/K 是可交换的，则 (1) 对 G/K 是真的，但对 G 不必为真．

(d) 若 G/K 是非交换的，则 (1) 对 G/K 不真，且对 G 不能真，因为 G 的关系是 G/K 的关系的一个子集．所以 G 也是非交换的．

练习 58 （148 页）： $x^2y^{-3} = I$ 推得 $x^2 = y^3$．再附加关

系 $x^2 = I$ 及 $(xy)^2 = I$ 以作成一个商群 G/K. 被扩大的关系集合对生成元 x 和 y 定义非交换群 D_3, 所以 G/K 是非交换群. 再根据练习 57 推得 G 也是非交换群.

练习 59 (156 页): 我们用 n_1 表示第一个循环中不同符号的个数, 用 n_2 表示第二个循环中不同符号的个数, 如此等等;所以 r 个循环中的不同符号的总个数是

$$n_1 + n_2 + \cdots + n_r = n.$$

第一个循环能表为 $(n_1 - 1)$ 个对换, 第二个循环能表为 $(n_2 - 1)$ 个对换,……, 第 r 个循环可表为 $(n_r - 1)$ 个对换, 所以总的对换数是

$$\begin{aligned}&(n_1 - 1) + (n_2 - 1) + \cdots + (n_r - 1)\\ &\quad = (n_1 + n_2 + \cdots + n_r) - r = n - r.\end{aligned}$$

练习 60 (158 页): 任何置换能表为循环的乘积, 而它们又可表为对换的乘积. 假设 (a_ja_k) 是任何与 (a_1a_2), (a_1a_3), $\cdots$, (a_1a_n) 不同的对换, 即 $a_j \neq a_1$ 及 $a_k \neq a_1$. 观察 $(a_ja_k) = (a_1a_j)(a_1a_k)(a_1a_j)$, 因为其右边意味着

$$a_1 \to a_j,\ a_j \to a_j,\ a_j \to a_1\ (\text{即 } a_1 \to a_1);$$

$$a_j \to a_1,\ a_1 \to a_k,\ a_k \to a_k\ (\text{即 } a_j \to a_k);$$

$$a_k \to a_k,\ a_k \to a_1,\ a_1 \to a_j\ (\text{即 } a_k \to a_j).$$

由此推得, 任何对换(因而任何置换)的乘积, 能表为仅包含 $n-1$ 个对换

$$(a_1a_2),\ (a_1a_3),\ \cdots,\ (a_1a_n)$$

的乘积.

练习 61 (161 页): 若 A_4 有 6 阶子群, 则它应有正规子群. 因为它的阶是 A_4 的阶的一半(见练习 52);但命题 (4)

指出 A_4 的正规子群的最大可能的阶是 4. 因此 A_4 没有 6 阶正规子群.

练习 62 (161 页): (a)$x^3=(abc)(abc)(abc)$ 意味着 $a\to b$, $b\to c$, $c\to a$ (即 $a\to a$); $b\to c$, $c\to a$, $a\to b$ (即 $b\to b$); $c\to a$, $a\to b$, $b\to c$ (即 $c\to c$).

(b) $x^2=(ab)(cd)(ab)(cd)$ 意味着 $a\to b$, $b\to b$, $b\to a$, $a\to a$ (即 $a\to a$), 等等.

练习 63 (174 页): 一个正 n 边形有 n 个相等的角及 n 个相等的边. 因为它的角的和是 $(n-2)180°$, 所以每个内角是 $(n-2)180°/n$. 假设有 k 个这样的 n 边形交于一个顶点 V, 因为平面是被覆盖的, 所以绕顶点 V 的 k 个内角的和是 360°, 所以

$$k\cdot\frac{n-2}{n}180°=360°,$$

由此得

$$k=\frac{2n}{n-2}.$$

$n\geqq 3$ 及 $k\geqq 1$ 的整数解 (n, k) 是: $n=3$, $k=6$; $n=4$, $k=4$; $n=6$, $k=3$. 为了看出没有其他的解, 可将上式改写为

$$k=\frac{2n}{n-2}=\frac{2}{1-\frac{2}{n}},$$

由此看到, 当 $n>6$ 时, 有 $2<k<3$.

练习 64 (180 页): "实线"三角形指出 $r^3=I$, 从"虚

线”三角形看出 $s^3=I$，六边形的边呈虚线与实线交错排列又指出 $(rs)^3=I$. 所以我们有关系

$$r^3=s^3=(rs)^3=I.$$

练习 65 (181 页)：每一个反射的周期为2，所以有 $a^2=b^2=c^2=I$. 这反射配对得到

正方形：$(bc)^2=I$，六边形：$(ac)^3=I$，十二边形：$(ab)^6=I$. 所以有

$$a^2=b^2=c^2=(bc)^2=(ac)^3=(ab)^6=I.$$